RISKNOWLOGY®

FUNCTIONAL SAFETY CERTIFICATION COURSE

Functional Safety for Safety Instrumented System Professionals and Engineers

Course Material

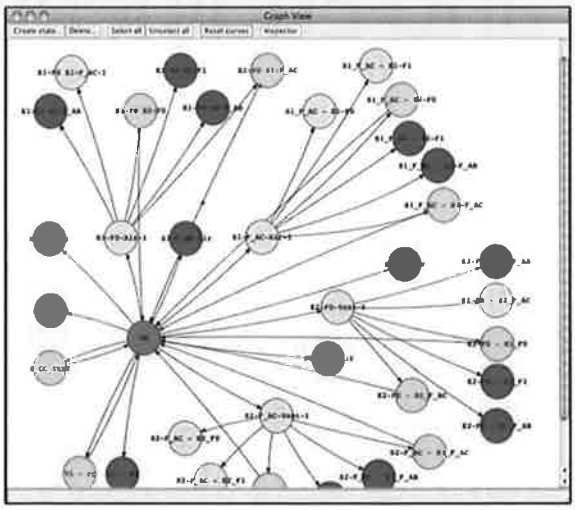
Risknowlogy offers a TÜV SÜD certified functional safety training course for safety instrumented system professionals and engineers.

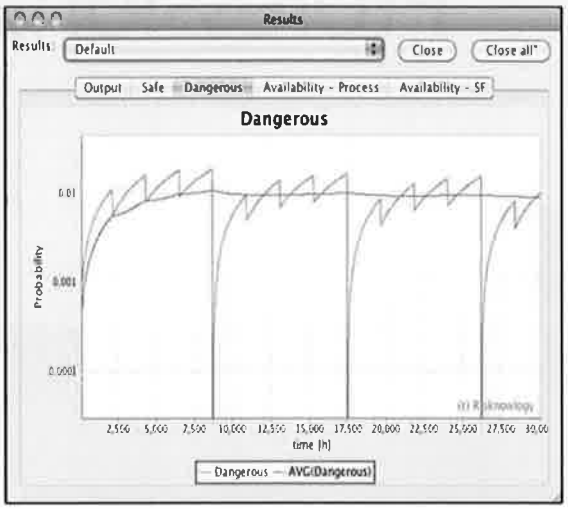
WWW.RISKNOWLOGY.COM

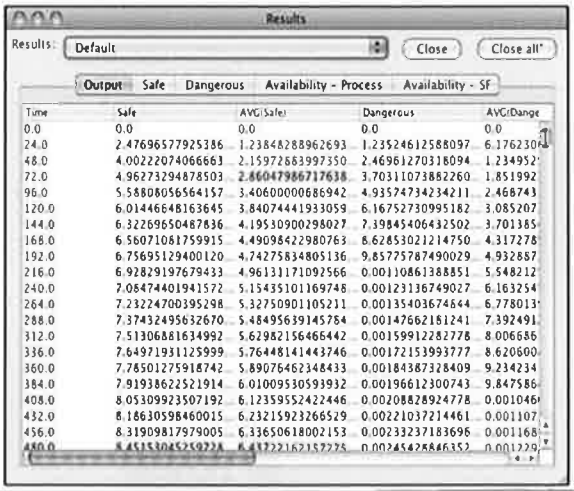
MARKOV MADE EASY
A PROBABILISTIC DECISION SUPPORT TOOL

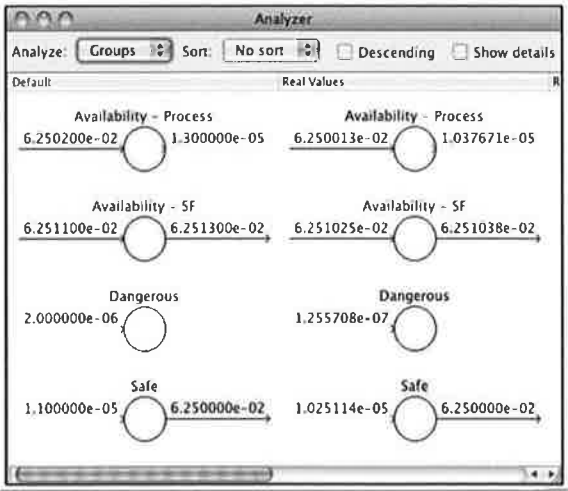
MARKOV is brought to you by Risknowlogy to make probabilitist calcualtions easy.

- Easy to learn and apply
- Model size is limited by memory only
- One model, multiple data sets to calculate
- Group your results
- Redistribute your probabilities at any time
- Use analyzers to inspect your model and the results
- Numerical and graphical results









Buy it online at www.risknowlogy.com/products

RISKNOWLOGY

EXPERTS IN RISK, RELIABILITY AND SAFETY

http://risknowlogy.com

RISKNOWLOGY®

Functional Safety Certification Course

Functional Safety for Safety Instrumented System Professionals

www.risknowlogy.com - riskfree@risknowlogy.com

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Objective

- The objective of this review course is to train the attendants in the fundamental principles of functional safety concerning safety-instrumented systems and to get their competency in the functional safety standards certified by TÜV

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Welcome

- In this module
  - Introduction
  - TÜV Functional Safety Certification Program
  - Course overview

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Introduction

- Nice to meet you…
  - Who are you?
    - Your name
    - Company
    - Position
    - Professional background
    - Why are you interested in **F**unctional **S**afety?
  - Who are we?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

During the Training…

- Please consider the following
  - In case of an emergency the exits are…
  - Feel free to answer your mobile phone but turn it to silent
  - Feel free to ask questions at any time

RISKNOWLOGY®

5

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

The Next Four Days

- Duration
  - 3 day course
  - Exam on the fourth day
- Working day
  - 9:00 – 16:30
  - 1 hour lunch at 12:00
  - Breaks at any time we want
- Exam
  - Duration: 4 hours

RISKNOWLOGY®

6

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Functional Safety Certification Program

- What is the program about?
  - The goal of the TÜV **Functional Safety Certification (FSC) program** is to establish around the world a group of functional safety professionals and experts with a common set of knowledge about functional safety according to important functional safety standards like IEC 61508, IEC 61511, IEC 62061 and so on.

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

The FSC Program Offers…

- Certification in the
  - Safety related systems for all systems
  - Automotive industry
  - Machinery industry
  - Process industry
  - Railway industry
- Courses for
  - Developers of hardware and software for safety devices
  - Users and integrators of safety devices

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Qualifications

- Two qualifications exist
  - Functional Safety Professional - FSP
  - Functional Safety Expert - FSE
- Training is conducted by an FSE

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Functional Safety Professional

- Requirements
  - 6 years of professional experience
  - Appropriate education gives you experience credit
    - Bachelor 2 years
    - Masters 3 years
    - PhD 4 years
  - Two references

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Course Overview

- Course
  - Modular with units
  - Exercises and examples
  - Discussions
- Exam
  - Closed book exam
  - 60 multiple choice questions
  - 25 open questions
- Passing criteria: Limit 75% score

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Contents

- Module:
  - Introduction to functional safety
  - The basics of functional safety
  - Hazard & risk analysis
  - Planning the safety instrumented systems
  - Hardware design
  - Software design
  - Certification, Proven In Use, Data
  - Using the safety instrumented systems
  - Conclusions

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Module 1

Introduction to Functional Safety

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Introduction to Functional Safety

- In this module
  - Accidents in the news
  - What is functional safety?
  - History functional safety
  - Overview laws & standards
  - Application area
  - Layers of protection
  - Safety instrumented system
  - Overview IEC 61508 / IEC 61511

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Directive
to way they should handle the hazard

Accidents in the News

- Well known accidents
  - Flixborough, UK, 1974
  - Seveso, Italy, 1976
  - Bhopal, India, 1984 largest in Nature 500,000, relase of Styrol
  - Piper Alpha, North Sea, 1988 after about 10 Years 5-8 released
- Recent accidents
  - Toulouse, France , 2001 September 21
  - Geleen, The Netherlands, 2003 April 1
  - Texas City, TX, USA, 2005 March 23
  - Jilin City, China, 2005 November 13
  - Buncefield, United Kingdom, 2005 December 11

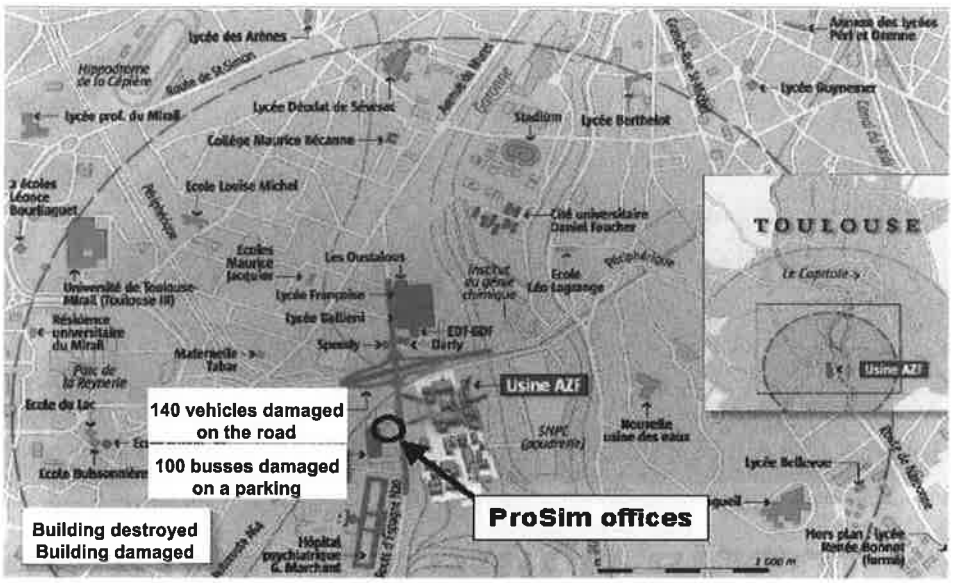
RISKNOWLOGY® 15 Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Toulouse

- Fact Sheet
  - Location: Toulouse, France
  - Date: 2001 September 21st
  - Problem: Explosion in a fertilizer plant equivalent to 20-40 tons TNT
  - Direct result:
    - 31 people were reported dead
    - 2,442 total number of injuries
    - 140 vehicles damaged on the road
    - 100 buses damaged on parking

RISKNOWLOGY® 16 Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Toulouse

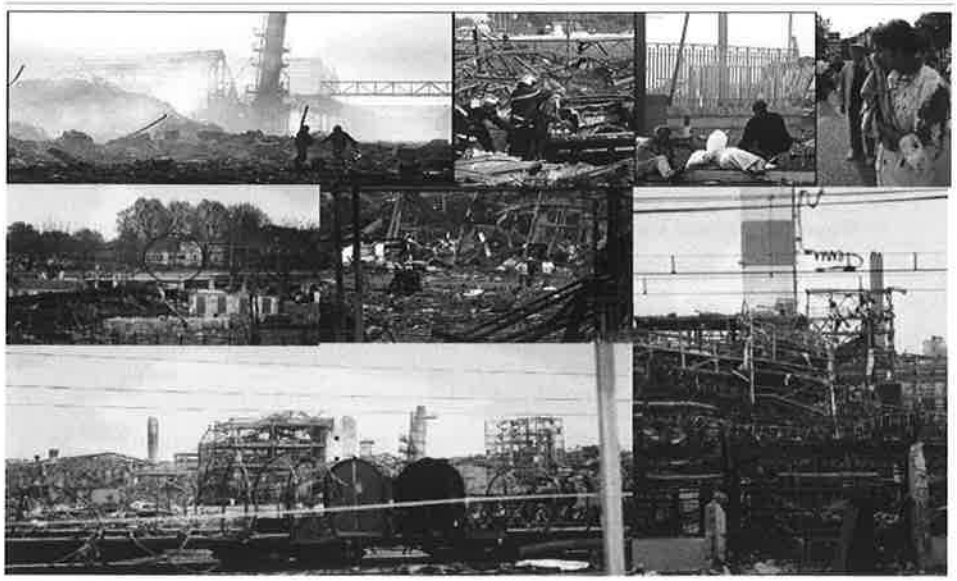


RISKNOWLOGY®

17

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Toulouse



RISKNOWLOGY®

16

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Toulouse

Figure 2 : View of the crater caused by the explosion

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Geleen – April 2003

- Fact Sheet
  - Location: Geleen, The Netherlands
  - Date: 2003 April 1st
  - Problem:
    - Several attempts had been made to start the furnace after maintenance
    - Operators in the control room let gas and air flow into the furnace
    - Explosion occurred because the furnace was still hot from previous startup attempts
    - Work instructions and procedures not followed during maintenance
    - No safety was built in during maintenance activities, safety completely depended on the operators during startup

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Geleen – April 2003

- Fact Sheet
  - Direct result:
    - 3 people killed
  - Indirect result:
    - DSM Melamine B.V. convicted
    - 75.000 Euro fine because they were responsible for the deaths
    - 25.000 Euro fine because they violated the law
    - Lawyer complained because the fine was in no relation to the profits made by DSM
    - Corporate damage: "Several 10 of millions of Euros" according to Lex Litjens (Director DSM Corporate Risk & Insurance)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Geleen – April 2003

Roof of the furnace, or what is leftover of it

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Texas City – Refinery Explosion

- Data
  - Location: Texas City, TX, USA
  - Problem: Several equipment failures, procedural failures
  - Direct results:
    - Probable cause was a failure in the rafinate splitter column
    - At least 5 explosions occurred
    - 15 killed, over 170 injuries
    - Buildings and cars destroyed
    - Residence shook up 5 miles from accident scene

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Texas City – Refinery Explosion

- Indirect results:
  - About 300 alleged violations were found in their safety rules
  - $ 21.3 Million Fine was paid to OSHA
  - $ 700 Million was reserved to compensate the victims
  - >3 Billion USD set aside for development over 5 years at US BP plants
- Between the lines
  - Over 100 incidents had been reported by BP over 6 years to the National Response Center (NRC)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Texas City – Refinery Explosion

Karen Warren / Chronicle

An aerial view of BP's Texas City refinery shows the flattened unit that exploded, seen in the foreground. The blast ripped a hole in a chemical storage tank 300 yards away, above center. The hole allowed benzene to evaporate into the air.

RISKNOWLOGY®

25

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Texas City – Refinery Explosion

RISKNOWLOGY®

26

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Jilin City – River Spill After Explosion

- Data
  - Location: Jilin City, China
  - Date: 2005 November 13
  - Problem: High levels of Benzene and Nitrobenzene spilled into river after explosion
  - Direct results: 6 people killed
  - Indirect results:
    - 80 km stretch of contaminated water
    - 40 hours to move through
    - But it was winter and the water was freezing
    - 6000+ people evacuated

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Jilin City – River Spill After Explosion

The leak was caused by a massive explosion at the PetroChina benzene factory in the city of Jilin on 13 November

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Polluted Water

Tests have shown concentrations of the carcinogenic chemical some 30 times higher than is considered to be safe

RISKNOWLOGY®

29

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

People Queuing

People in Harbin, north-eastern China, queue for water after the city's own supplies were contaminated by the benzene leak

RISKNOWLOGY®

30

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Buncefield - Oil Depot

- Data
  - Location: Buncefield, United Kingdom
  - Problem: Overfilling tank due to equipment failure, leading to vapor cloud which got ignited
  - Direct results:
    - Explosion lead to a large fire which took 5 days
    - 23 storage tanks caught fire
    - 43 people injured
    - 2000 people evacuated
    - Estimated economic impact 1 Billion British Pound

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Buncefield - Oil Depot

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Buncefield - Oil Depot

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

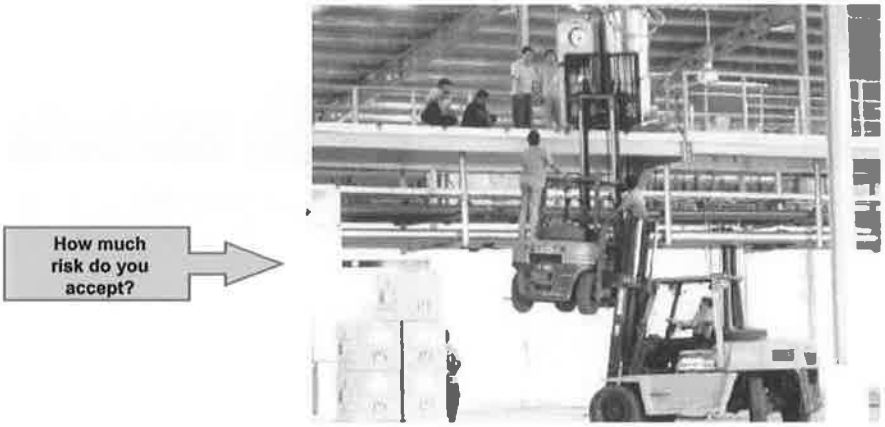
Safety Expensive?

- Why should we invest in safety?
  - You think safety is expensive, try an accident…
  - Today an accident cost more than 10x the investment in the process
  - We have had terrible accidents in the past
  - We learned, but accidents with serious impact still happen today
- Training is one way to help people become more aware and knowledgeable about safety

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What is Safety?

- ISO/IEC guide 51 defines safety as
  - Freedom from unacceptable risk



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Legal Status IEC 61511

- Standards are never legally binding, merely they are used for guidance, but ...
- Since its release (2003) IEC 61511 is considered State-of-the-Art or Good Engineering Practice
- State-of-the-Art means IEC 61511 is
  - Technically feasible and applicable
  - Organizationally possible to plan
  - Economically feasible
- State-of-the-Art is a legal term in Europe and is the only thing court looks at
- This makes it almost impossible not to comply to IEC 61511 when it comes to safety instrumented systems

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Overview Laws

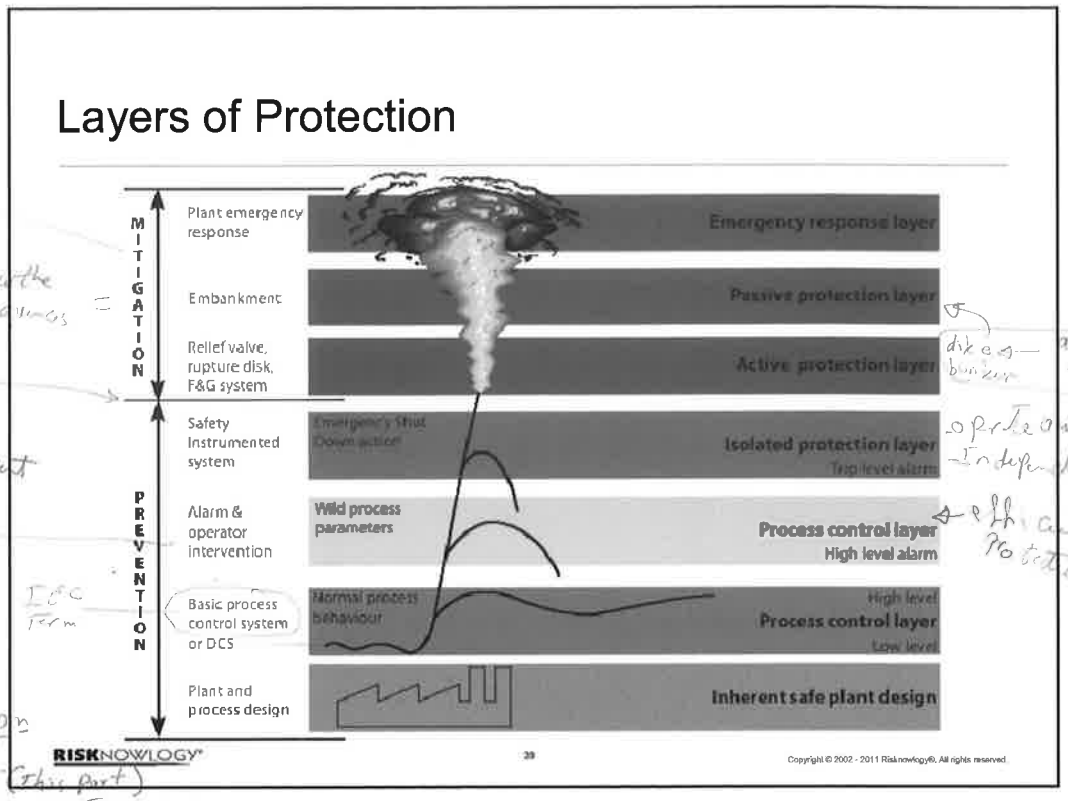
- In Europe many Directives (Laws) exist for example:
  - Medical Directive
  - Lift Directive
  - Seveso II Directive
  - Machinery Directive
  - ATEX Directive
  - PED Directive
- In the USA
  - EPA: risk management program - 40 CFR part 68
  - OSHA: process safety management - OSHA §1910.119

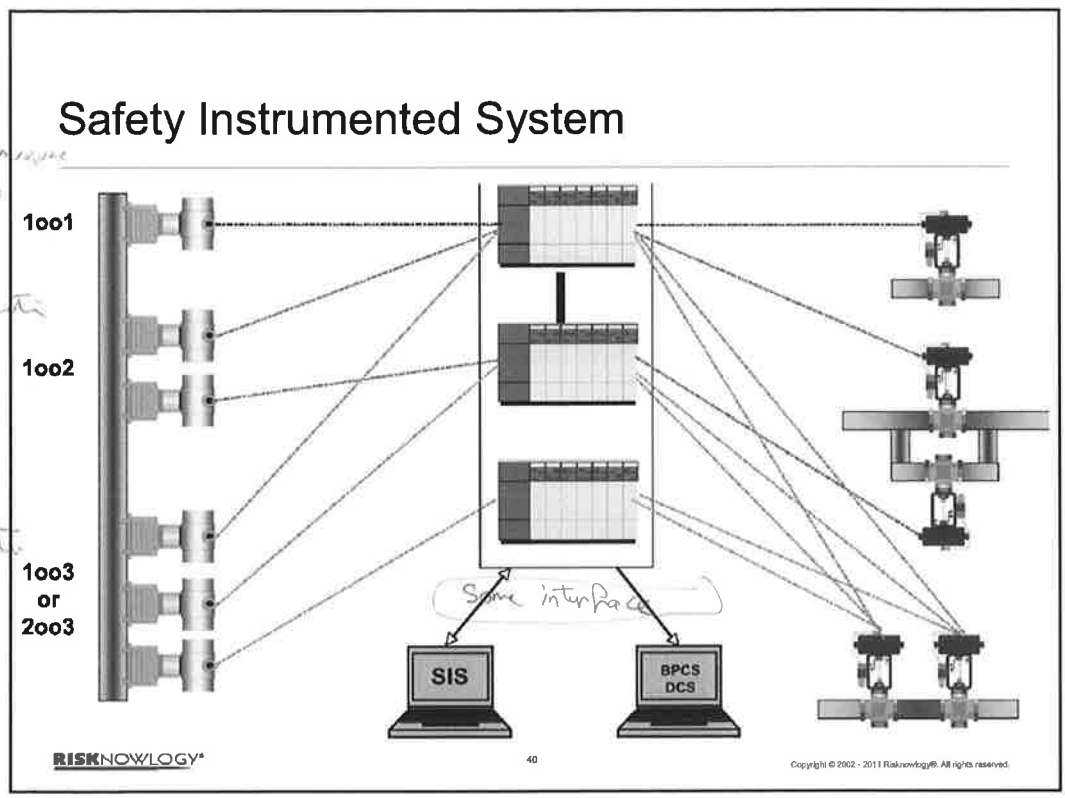
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Overview Laws

- How about in your country?
  - Do you have local occupational safety and health laws?
  - Do you have national standards that you need to apply?
  - How does IEC 61511 fit into these laws?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.


Layers of Protection
MITIGATION
PREVENTION
Plant emergency response
Emergency response layer
Embankment
Passive protection layer
Relief valve, rupture disk, F&G system
Active protection layer
Safety Instrumented system
Isolated protection layer
Alarm & operator intervention
Wild process parameters
Process control layer
High level alarm
Basic process control system or DCS
Normal process behaviour
High level
Process control layer
Low level
Plant and process design
Inherent safe plant design
RISKNOWLOGY
39
Copyright © 2002 - 2011 Risknowlogy®, All rights reserved.


Safety Instrumented System
1oo1
1oo2
1oo3
or
2oo3
SIS
BPCS
DCS
RISKNOWLOGY
40
Copyright © 2002 - 2011 Risknowlogy®, All rights reserved.

Safety Integrity Level - SIL

- SIL is how we measure the performance of safety functions carried out by safety instrumented systems
- SIL has 3 sides to the story
  - Process owners:
    Which safety functions do I need and how much SIL do I need? Design
  - Engineering companies, system integrators, product developers:
    How do I build SIL compliant safety devices, functions or systems?
  - Process operators:
    How do I operate, maintain and repair safety functions and systems to maintain the identified SIL levels?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Integrity Level - SIL

- There are 4 SIL levels in IEC 61511 and IEC 61508
  - SIL 1, 2, 3 and 4
- Important SIL properties
  - Applies to the complete safety function / loop every element of the safety loop should comply with the req. SIL
  - There are technical and non-technical requirements defined per SIL level
  - Higher SIL means
    - Stricter requirements
    - The safety function fails less and is thus more available

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Integrity Level - SIL

- Most famous SIL requirements is the Probability of Failure on Demand

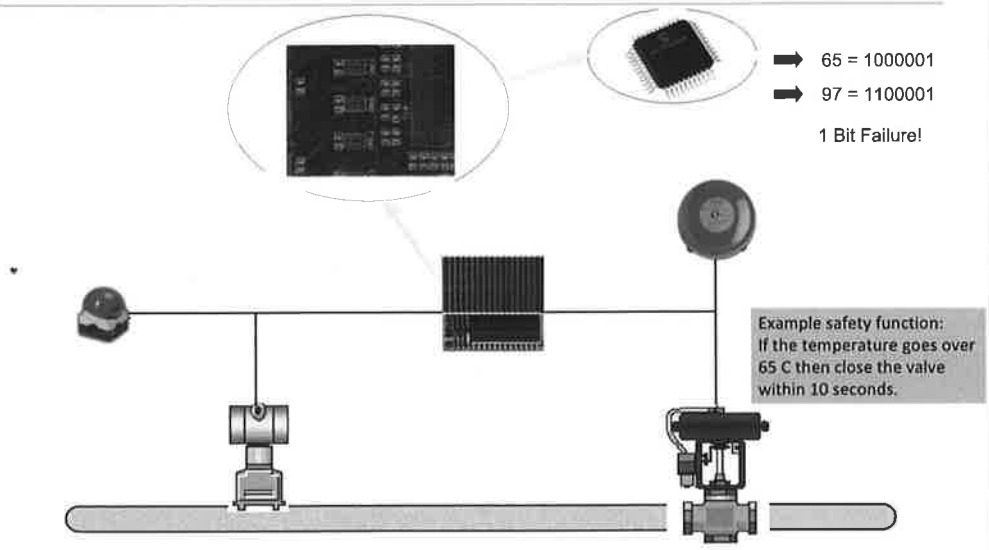
SIL	PFDavg	Safety Availability	Risk Reduction
4	0.0001 - 0.00001	0.9999 - 0.99999	10000 - 100000
3	0.001 - 0.0001	0.999 - 0.9999	1000 - 10000
2	0.01 - 0.001	0.99 - 0.999	100 - 1000
1	0.1 - 0.01	0.9 - 0.99	10 - 100

RISKNOWLOGY®

43

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Problems With Safety Instrumented Systems



RISKNOWLOGY®

44

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Instrumented Systems States

- A safety instrumented system can be in 4 different states
  - **Ok**: no internal failures
  - **Safe**: the safety instrumented systems fails in a way that the safety function is carried out without a demand
  - **Dangerous**: the safety instrumented systems fails in a way that the safety function cannot be carried out in case of a demand
  - **Intermediate**: safety function can still be carried out despite one or more internal safety instrumented systems failures

Spurious Trip
Tolerate, Time To repair

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

SIS Versus Process

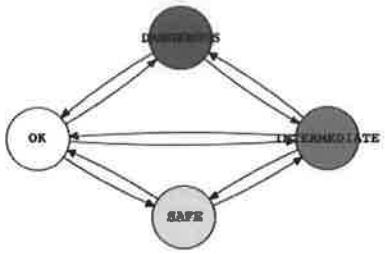
SIS States	Process to be protected
Ok	Process is available
Safe	Process has tripped
Dangerous	Process is available but not protected
Intermediate	Process is available, SIS is available, but it is time to repair it

PFD tells you what the probability to be here

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Instrumented System Failures

- Safety instrumented systems can fail because of…
  - Random hardware failures
  - Common cause hardware failures
  - Systematic failures
- Any of these failures puts the safety instrumented system into a specific system state
  - Safe
  - Dangerous
  - Intermediate



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Random Hardware Failures

- Definition
  - A spontaneous failure of a hardware component at any given time
    - Permanent – exist until repaired
    - Dynamic – exists only under certain circumstances
- IEC 61508 approach
  - Measures to control failures
  - Hardware qualitative and quantitative (PFDavg, PFH) reliability study

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

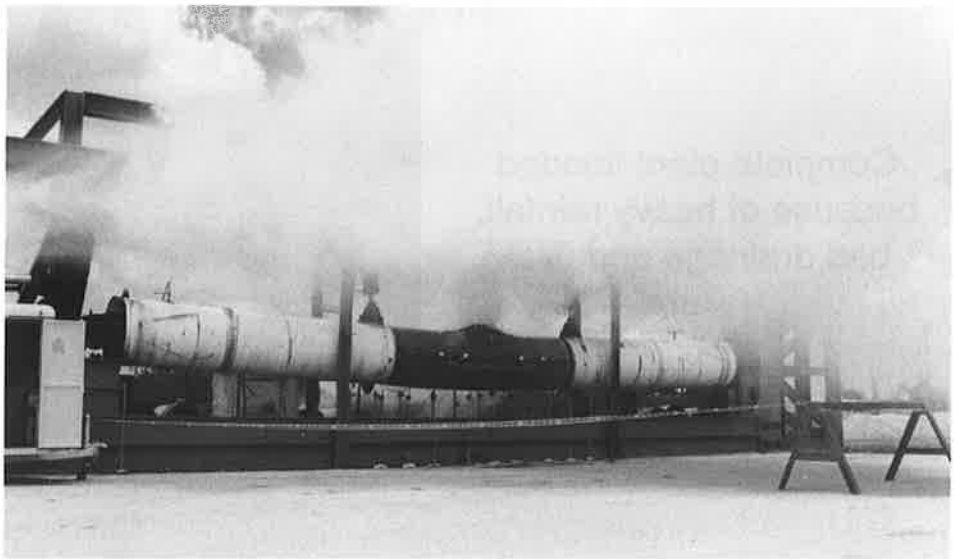
Measures To Control Failures

Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	M	M	M	M
Separation of electrical energy lines from information lines	M	M	M	M
Increase of interference immunity	M	M	M	M
Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	M	M	M	M
Program sequence monitoring	HR	HR	HR	HR
Measures against temperature increase	HR	HR	HR	HR
Spatial separation of multiple lines	HR	HR	HR	HR
Idle current principle (where continuous control is not needed to achieve or maintain a safe state of the EUC)	R	R	R	R
Measure to detect breaks and shorts in signal lines	R	R	R	R
Failure detection by on-line monitoring	R	R	R	R
Tests by redundant hardware	R	R	R	R
Code protection	R	R	R	R
Antivalent signal transmission	R	R	R	R
Diverse hardware	-	-	-	R
Software architecture	See Tables A.2 and C.2 of IEC 61508-3			

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Random Hardware Failure Example



RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Common Cause Hardware Failures

- Definition:
  - Failures which result from events causing simultaneous or coincident failures of two or more separate channels in a multiple channel system leading to system failure
  - These events are related to the environment (heat, EMC, flooding, ...)
- IEC 61508 approach
  - Diversity as a measure to control failures
  - Take into account during quantitative reliability analysis (PFDavg, PFH)

RISKNOWLOGY®

51

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Common Cause Does Not Happen?

Complete plant flooded because of heavy rainfall, bad drainage and dike failure

RISKNOWLOGY®

52

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Is diverse will overcome systematic failures ???

Systematic Failures

- Definition
  - A hidden fault in design or implementation
    - Software as well as hardware
    - Design specifications
    - User manuals
    - Procedures, etc
  - Can occur in any lifecycle phase
- IEC 61508 approach
  - Measures to avoid failures
  - NOTE: not included in the quantitative reliability analysis (PFDavg, PFH)

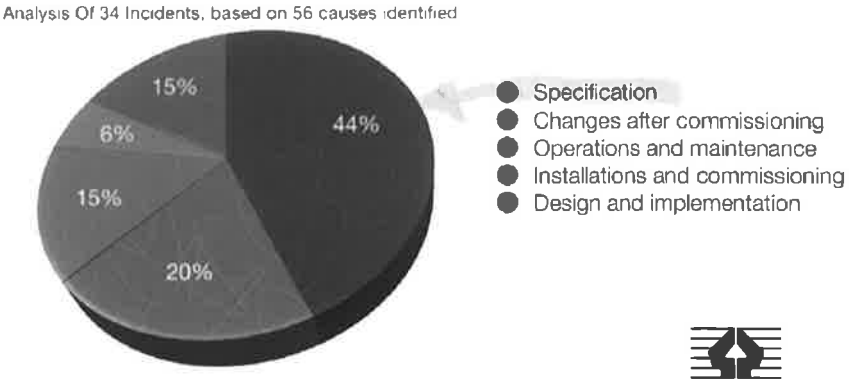
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Measures To Avoid Failures

Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
Project management	M	M	M	M
Documentation	M	M	M	M
Separation of E/E/PE system safety functions from non-safety functions	HR	HR	HR	HR
Structured specification	HR	HR	HR	HR
Inspection of the specification	-	HR	HR	HR
Semi-formal methods	R	R	HR	HR
Checklists	R	R	R	R
Computer aided specification tools	-	R	R	R
Formal methods	-	-	R	R

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

When Do Failures Occur?



Out of control: Why control systems go wrong and how to prevent failure? (2nd edition, source: © Health & Safety Executive HSE – UK)

HSE Health & Safety Executive

RISKNOWLOGY®

55

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

One Final Note

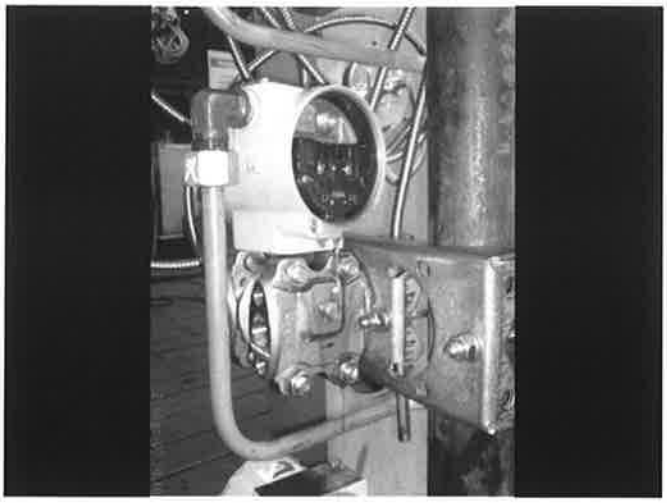
- Common cause versus systematic failures
  - When a common cause event takes place all same devices fail at the same time
  - When a systematic failure exists all same devices fail at the same time
  - In other words, the effect of a common cause or systematic failure is the same on safety function level, i.e., the safety function fails
  - We make a difference between common cause and systematic failures because we need to take away the cause in a different way
- Common cause: Solution could be diversity - measures to control failures
- Systematic: Solution could be changing procedures or more testing, etc - measure to avoid failures
- So we deal with the same problem (losing the safety function) in a different way

RISKNOWLOGY®

56

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Or Maybe We Do ....



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

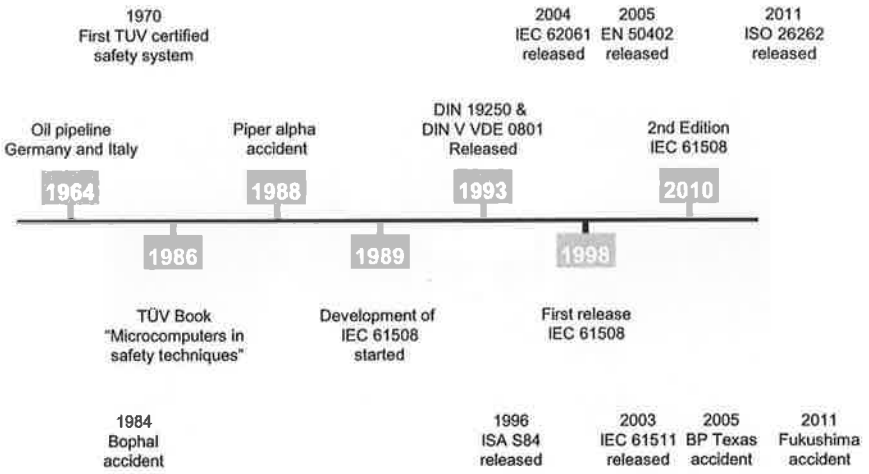
What Is Functional Safety?

- A safety instrumented system is 100% functionally safe if
  - All ***random***, ***common cause*** and ***systematic*** failures do **not** lead to malfunctioning of the safety system and do not result in
    - Injury or death of humans
    - Spills to the environment
    - Loss of equipment or production
- 100% functional safety does not exist but SIL 1, 2, 3 or 4 does

Reach To a degree which is accepted

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

History Functional Safety



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Functional Safety Standards

- For safety instrumented systems there are two important standards when it comes to functional safety:
  - IEC 61508 - Functional safety of electrical / electronic / programmable electronic safety-related systems
    - IEC 61511 == ANSI/ISA 84.00.01 - Functional safety: safety instrumented systems for the process industry sector

- specific for process industry
- any Tech.
- regardless any Tech.

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Overview IEC 61508

- **Part 1: General requirementsPart 2: Requirements for Electrical, Electronic, Programmable Electronic Systems (E/E/PES)Part 3: Software requirementsPart 4: Definitions and abbreviations**Part 5: Examples of methods for the determination of safety integrity levels (SIL)Part 6: Guidelines on the application of Parts 2 & 3Part 7: Overview of techniques and measures

1, 2, 3 & 4

5, 6, 7 not standard

IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION
PUBLICATION FONDAMENTALE DE SÉCURITÉ

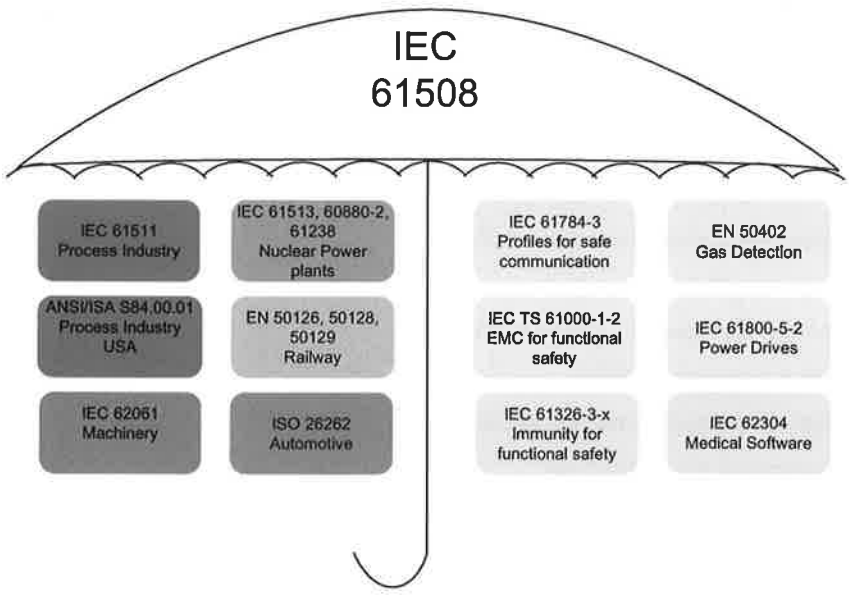
Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 1: Exigences générales

RISKNOWLOGY®

61

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved



RISKNOWLOGY®

62

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Application Area IEC 61508

- IEC 61508 applies:
  - To any electrical / electronic / programmable electronic (E/E/PE) safety related systems Specific technology regardless the industry
  - Especially where no functional safety standard exists
  - Anywhere in the world where it is accepted

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Application Area IEC 61508

- Typical applications are
  - Programmable electronic system (PES)
  - Safety instrumented systems (SIS)
  - Emergency shutdown systems (ESD)
  - High integrity pressure protection systems (HIPPS)
  - Burner management systems (BMS)
  - Fire & gas system (F&G)
  - High speed over protection system
  - Emergency brake of a train
  - Any other names?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Overview IEC 61511

- **Part 1: Framework, definitions, system, hardware and software requirements**
- Part 2: Guideline for the applications of IEC 61511-1
- Part 3: Guidance for the determination of the required safety integrity levels

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

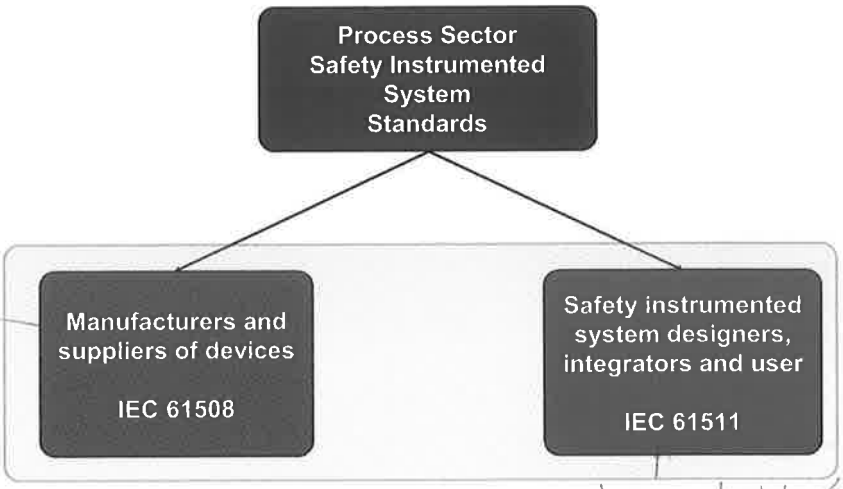
Application Area IEC 61511

- IEC 61511 applies to safety instrumented systems
  - Instruments (E/E/PE or not)
  - Logic solver (E/E/PE or not)
  - Actuators (E/E/PE or not)

Two Key concepts for SIL
① SIL
② Safety life cycle

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

IEC 61508 Versus IEC 61511



RISKNOWLOGY®

67

Copyright © 2002 - 2011 RISKNOWLOGY®. All rights reserved.

Exercise # 01

- See exercises printout
- Which failure categories exist
- Classify failures

RISKNOWLOGY®

68

Copyright © 2002 - 2011 RISKNOWLOGY®. All rights reserved.

Summary Module 1

- What we learned…
  - We now know what functional safety is
  - Where it is coming from
  - What layers of protection are two Layers provd mitigation Prevation is Mitigation is
  - What SIL is all about to which degree sys is trustable, how this will be available, how sz wtr reduce the risk
  - What are the practical problems with safety instrumented systemss
  - And we got to know the two most important functional safety standards in our industry

Techn'l non Techn., to whole loop

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

The Basics of Functional Safety

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

The Basics of Functional Safety

- In this module
  - Functional safety management
  - Lifecycle concept
  - Documentation
  - Implementation and monitoring
  - Verification, validation, assessment and audits
  - Modifications
  - Competency

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Why Manage Safety?

What Went Wrong?

- So why do we actually want to manage safety?
  - Safety should be the only outcome of a project
  - Safety should not be a lucky shot
  - Safety should be traceable and repeatable

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Functional Safety Management

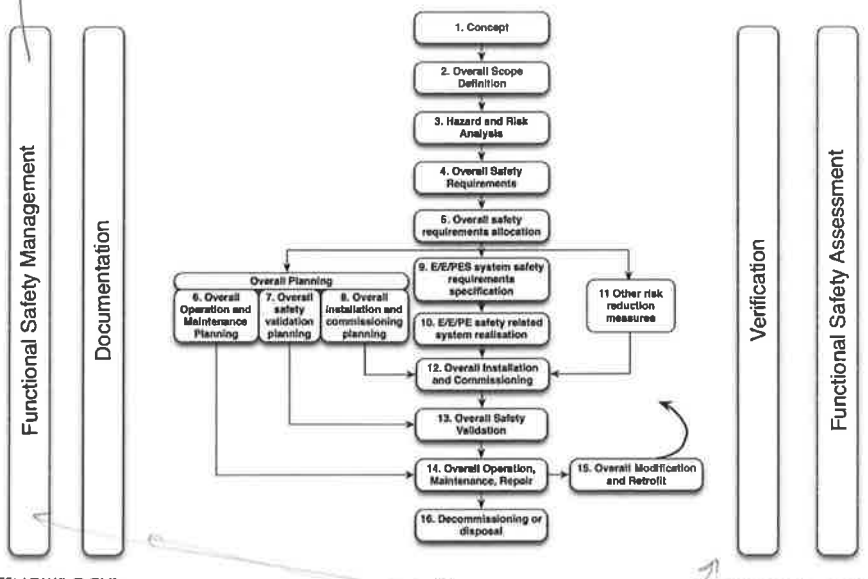
- Objectives are twofold
  - Define all technical and management activities during the lifecycle of the safety instrumented systems
  - Specify responsibilities or activities for
    - Persons
    - Departments
    - Organizations

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlegy®. All rights reserved.

IEC 61508 Lifecycle Concept

16 Phases


Functional Safety Management
Documentation
1. Concept
2. Overall Scope Definition
3. Hazard and Risk Analysis
4. Overall Safety Requirements
5. Overall safety requirements allocation
Overall Planning
6. Overall Operation and Maintenance Planning
7. Overall safety validation planning
8. Overall installation and commissioning planning
9. E/E/PES system safety requirements specification
10. E/E/PE safety related system realisation
11 Other risk reduction measures
12. Overall Installation and Commissioning
13. Overall Safety Validation
14. Overall Operation, Maintenance, Repair
15. Overall Modification and Retrofit
16. Decommissioning or disposal
Verification
Functional Safety Assessment

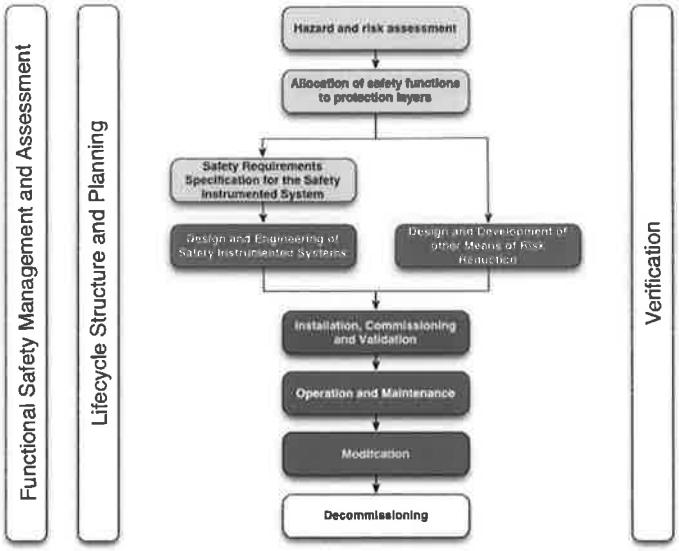
RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlegy®. All rights reserved.

the value to having safety lifecycle model is it is systematic

in each phase will do 4 Tasks @ each phase.
don't go to next phase before carry out these 4 activities

IEC 61511 Lifecycle Concept


Functional Safety Management and Assessment
Lifecycle Structure and Planning
Hazard and risk assessment
Allocation of safety functions to protection layers
Safety Requirements Specification for the Safety Instrumented System
Design and Engineering of Safety Instrumented Systems
Design and Development of other Means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning
Verification

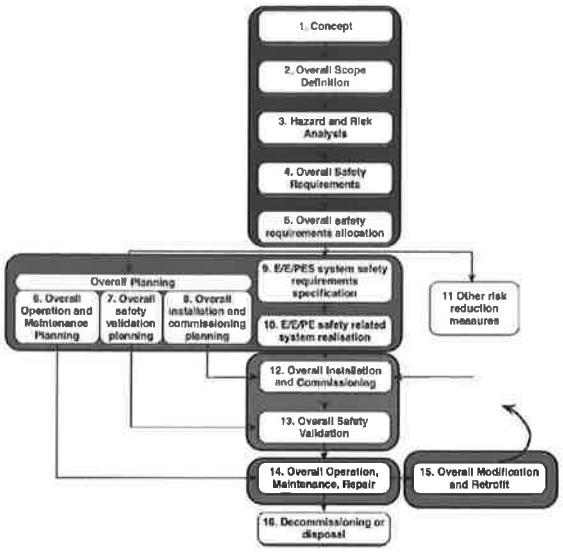
Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

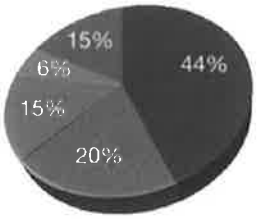
Lifecycle Concept

- A lifecycle helps us in a systematic way to
  - Identify activities that need to be carried out
  - Identify required expertise/competencies per phase
  - Identify the documentation requirements to carry out the activities
  - Deal with responsibilities for these activities
  - Deal with FSM, V&V, assessment and audit activities
- In practice different lifecycles are used by different stakeholders
  - End-users, integrators, developers, hardware, software …
- In practice somebody needs to manage this...

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Lifecycle & Frequency of Failures


1. Concept
2. Overall Scope Definition
3. Hazard and Risk Analysis
4. Overall Safety Requirements
5. Overall safety requirements allocation
Overall Planning
6. Overall Operation and Maintenance Planning
7. Overall safety validation planning
8. Overall installation and commissioning planning
9. E/E/PES system safety requirements specification
10. E/E/PE safety related system realisation
11 Other risk reduction measures
12. Overall Installation and Commissioning
13. Overall Safety Validation
14. Overall Operation, Maintenance, Repair
15. Overall Modification and Retrofit
16. Decommissioning or disposal



- Specification
- Changes after commissioning
- Operations and maintenance
- Installations and commissioning
- Design and implementation

RISKNOWLOGY®

77

Copyright © 2002 - 2011 Risknowlogy®, All rights reserved

Documentation

- Why should safety be documented?
  - We work in lifecycle phases, we need to pass on information to different engineering disciplines
  - Documentation needs to exist for the purpose of
    - Carrying out the work
    - Verifying the work
    - Assessing the work
    - Auditing the work

RISKNOWLOGY®

78

Copyright © 2002 - 2011 Risknowlogy®, All rights reserved.

Safety Manual How to use equipm to keep safety integrity in all lifecycle

Documentation

- Documentation should
  - Be accurate
  - Be easy to understand
  - Suit the purpose for which it is intended
  - Be available, accessible, maintainable
- Documentation should be formally controlled
  - Title, author, date, revision index
  - Reviews and approval
  - Traceability to requirements
  - Etc

Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

Typical Documentation

Phase	Information
All phases	Planning documents: e.g., safety plan, verification plan
Hazard and risk analysis	P&ID's, PFD, Material Data Sheets, Equipment Information, HAZOP, FMEA, FTA, LOPA
Safety requirements	Specifications: safety functions, systems, equipment and their properties
Realization	System design, hardware design, software design, layout, circuit diagrams, manuals, PFD/PFS calculations & data
Overall installation and commissioning	Checklists, test report of installation and commissioning
Overall safety validation	Validation plan, FAT, SAT test results
Overall operation and maintenance	Logs, audit reports, spurious trip reports, demand reports, proof tests
Overall modification and retrofit	Modification request, impact analysis report, approval statement, re-verification test reports

Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

Implementation and Monitoring

- Performance of the SIS depends on having the right procedures
  - Procedures to handle recommendations from
    - Hazard and risk analysis
    - Assessments and audits
    - Verification
    - Validation
    - Post incident activities
  - Procedures how to deal with suppliers of products and/or service
  - Procedures monitoring that the original safety requirements are still valid as maybe process change due to ...zing on

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

V&V, Assessments, Audits

- A few important terms often misunderstood
  - Verification
  - Validation
  - Assessments
  - Audits

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Verification Versus Validation

- Both verification and validation means we are testing something
- What is verification?
  - Did I build the **product/system correct**?
  - Did I carry out the **procedure correct**?
  - Verification is carried out after each lifecycle phase
- For example
  - Requirement for system integrator:
    Select correct safety instrumentation for a SIL 2 loop
  - Verification activity:
    Engineer verifies for each piece of equipment the safe failure fraction, hardware fault tolerance, software, environmental conditions, etc.

- Technical Tasks
- design review phase

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Verification Versus Validation

- What is validation?
  - Did I build the **correct product/system**?
  - Did I use the **correct procedure**?
  - Validation is a phase in the lifecycle
  - Validation needs to be verified
  - Validation is carried out by the "customer": Did I receive what I ordered?
- For example:
  - End-user requirement: Build a SIL 2 emergency shutdown function function
  - Validation activity: End-user performs Site Acceptance Tests (SAT)

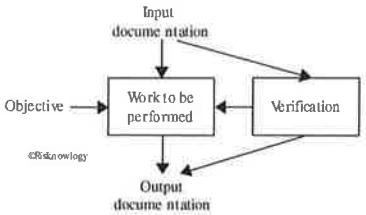
Validation is the SAT

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

FAT maybe Verification

Verification

- IEC 61508
  - confirmation by examination and provision of objective evidence that the requirements have been fulfilled
- IEC 61511
  - activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase



How to Confirm & demonstrate

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

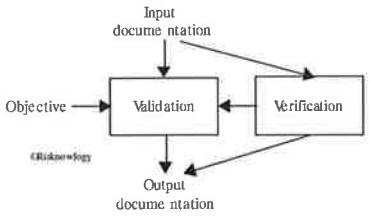
How We Do Verification in Practice

- Verification depends on the work to be performed in the lifecycle phase
  - Visual inspection of a P&ID
  - Review meetings
  - HAZOP, FMEAs, SIL calculation reports
  - List of open points
  - Etc.
- Verification is done
  - By testing, simulation, analysis …
  - By product suppliers and third parties
  - By everybody and for everything

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Validation

- IEC 61508
  - confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled
- IEC 61511
  - activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification



RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

How Do We Do Validation in Practice?

- Validation is performed on the real safety instrumented system
- Validation is done
  - By testing, simulation, visual inspection, …
  - To check whether we received what we ordered
- Validation should be done
  - By the end-user of the safety instrumented system
- For safety instrumented systems validation is typically done via a
  - Factory Acceptance Test - FAT - partial validation
  - Site Acceptance Test - SAT - full validation
- Validation needs to be verified
  - Review filled out checklists
  - Review FAT/SAT reports

RISKNOWLOGY®

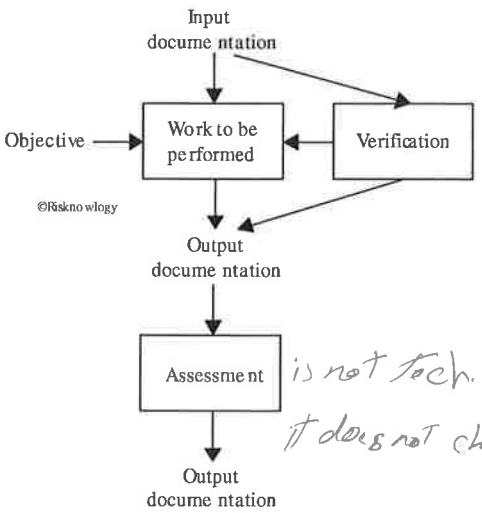
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Verification and/or Validation Activities

- For both verification and validation we need to
  - Plan the tests
  - Perform the tests, and
  - Document the results of the tests
    - What is the basis for testing?
      - For validation this is the safety requirements specification (SRS)
    - What are we testing?
    - Who is testing?
    - What tools/techniques/equipment is needed to test?
    - What pass/fail criteria do we have?
    - How to handle non-compliances?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Overview



is not tech. Task ; it is review
it does not check Technical details

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

assessment to be carried out each phase with external resources

About Assessments

it is an inspection

- Why do we need assessments?
  - The Assessor checks whether the people did what we ask them to do
- What does an Assessor try to answer?
  - Which lifecycle was applied?
  - Did we select competent people for the activities?
  - Where the people formally trained?
  - Is the input documentation for each lifecycle phase defined?
  - Did we produce the appropriate output documentation?
  - Did we follow up on previous recommendations?
  - Did the responsible, e.g., the system integrator, follow the plan?
  - Etc.

RISKNOWLOGY® 91 Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

Audit is an Assessment in long term (long Phase)

Functional Safety Assessment

- Functional safety assessment(s) (FSA)
  - Check whether everything was carried out as it was planned to be carried out not Tech. details
  - Are carried out for each phase of the lifecycle or a combination of phases
  - Are carried out with sufficient independence
- What is it not?
  - Is not the same as V&V
  - Does not verify the technical content in detail

Verification is technical details activities

RISKNOWLOGY® 92 Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

Level of Independence - IEC 61508

- Independence applies to assessment and audits, not V&V activities, according to IEC 61508

Minimum Level of Independence	Safety Integrity Level			
	1	2	3	4
Independent person	X	X^1	Y	Y
Independent department	-	X^2	X^1	Y
Independent organization	-	-	X^2	X

- = not necessary
Y = not sufficient
X = sufficient

X^1 = If X^2 applies then X^1 should be read as NR
X^2 = Applies if less previous experience, more complexity, novelty of design, newer technology, etc.

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

after Validation

Audits

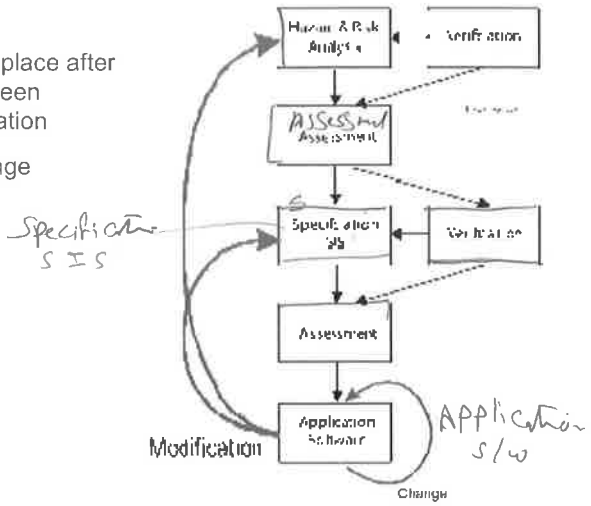
For long phase (odM "20+ years")
To keep SIL level without degratation

- Audits are similar to assessments
  - Basically it is a periodically performed assessment
  - Applies to "long" lifecycle phases like the operation, maintenance and repair phase
- Additionally audit procedures are required
  - Frequency of audits
  - Recording and follow-up
- Same independence applys between people doing the work and people performing the audits

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Modifications

- What is a modification?
  - Any change that takes place after a lifecycle phase has been completed is a modification
  - Anything else is a change



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Modifications Need to Be Managed

- A modification procedure needs to be defined upfront
- Why do we need to manage modifications?
  - We need to understand the impact of the desired modification, do we need to
    - Adjust a safety limit in software?
    - Replace a safe device with another one of a different brand?
    - Change the architecture of safety loop?
    - Redo testing? How much testing needs to be redone?
    - Redo documentation? Which documentation?
    - Etc

Inform people (any people)
Train people.

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Don't Just Start Making Modifications

- You always need to follow the modification procedure
  - Only qualified and properly trained personnel are allowed to perform modifications
  - Request the desired modification, which will address the following:
    - What is the reason for the change?
    - What hardware and/or software needs to be changed?
    - Which hazards are affected?
  - Request is send to the Modification team for approval
  - Start an Impact Analysis

Copyright © 2009 - 2011 Risknowlogy®. All rights reserved

Impact Analysis

- An impact analysis includes:
  - An assessment on what impact the change has
  - A hazard and risk analysis to understand which, and to what, extend lifecycle phases are affected
  - A guarantee of functional safety at all times and to the SIL required
- Impact analysis is send to the Modification team for review
- Result of the impact analysis determines whether the modification will be authorized

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Modification Documentation

- What needs to be documented?
  - The modification or retrofit request including a description of the modification
  - The hazards that might be affected due to this modification
  - The impact analysis
  - The modification's approval
  - The actual work performed
  - Re-verification and revalidation of data and results
  - All documents affected by the modification and retrofit activity

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Competency of People

- Competency should measure
  1. Knowledge
  2. Formal training
  3. Experience
- In the area of
  - Application
  - Technology
  - Standards, regulations, law
- Competency should be periodically refreshed, updated and continuously assessed

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 02

- Verification of a safety requirement specification
  - What do we verify when we verify...

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 03

- Case study: Accident Documentary
  - Next a documentary is shown
  - Write down everything that has gone wrong during this accident and that has to do with ***functional safety management***

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Summary Module 2

- Summary
  - Basics of functional safety starts with good management
    - Functional safety management
    - Lifecycle
    - Documentation
    - Verification & validation, assessment, and audits
    - Modification
    - Competency
  - Have the right people, do the right work, at the right time, using the right tools and the right techniques

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard & Risk Analysis

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard & Risk Analysis

- In this module:
  - How much safety is enough?
  - Risk management
  - Hazard identification
  - Hazard analysis
  - Risk reduction
  - Techniques
  - Risk graph, risk matrix
  - Identification safety functions

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Where Are We?

Hazard and risk assessment
Allocation of safety functions to protection layers
Safety Requirements Specification for the Safety Instrumented System
Design and Engineering of Safety Instrumented Systems
Design and Development of other Means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

HRA Nomenclature

- Many different names exist in this industry
  - AHA - Area Hazard Analysis
  - HAZID – Hazard Identification Analysis
  - HAZAN – Hazard Analysis
  - HAZOP - Hazard and Operability Analysis
  - LOPA - Layers of Protection Analysis
  - OHA - Operability Hazard Analysis
  - PHA – Process Hazard Analysis
  - QRA – Quantitative Risk Analysis
- Any other names you have heard?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Is a Hazard?

- Definitions
  - A substance, object or situation that can give rise to injury or damage (Kletz)
  - An inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment (AIChE)
  - Potential source of harm (IEC 61508/61511)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Is a Hazardous Event?

- An hazardous event occurs when the potential hazard has happened
- Also referred to as hazardous scenario

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Is Risk?

- The risk we talk about is related to a hazard
- Risk is a combination of
  - The severity of consequences (C)
  - The frequency of occurrence (F)
  - Risk = C x F
- We need to determine the risk associated with the hazardous event

- don't think about now
- it is chain of one break, person will Brake right + left

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Is Tolerable Risk?

there is no zero risk

- The basis of risk analysis: **tolerable risk**
  - How much risk do you tolerate?
  - How can we estimate how much risk reduction we need if we do not know how much we tolerate?
- Who determines tolerable risk? Society does...
  - Risk of smoking
  - Risk of driving a car
  - Risk of doing business

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Tolerable Risk

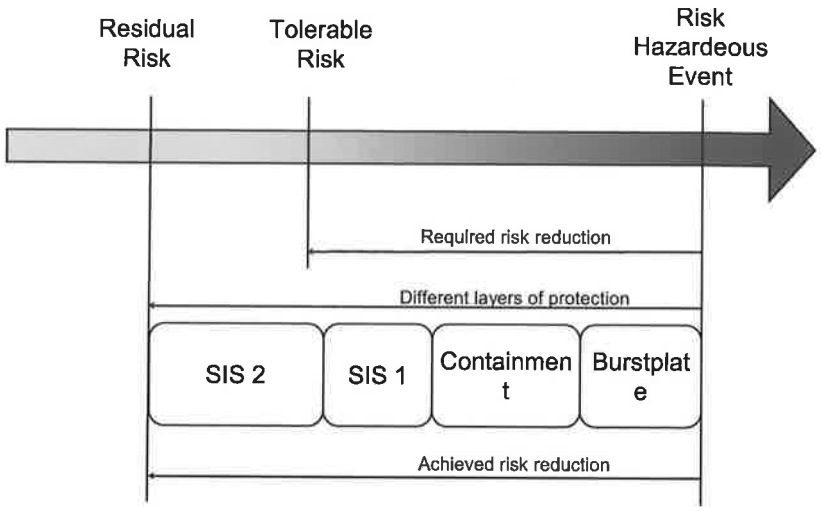
- How governments think about us:

Country	Maximum risk to the public
UK	1×10^{-4}
Hong Kong	1×10^{-5}
Netherlands	1×10^{-6}
Australia	1×10^{-6}
Germany	0

Source: CCPS

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction

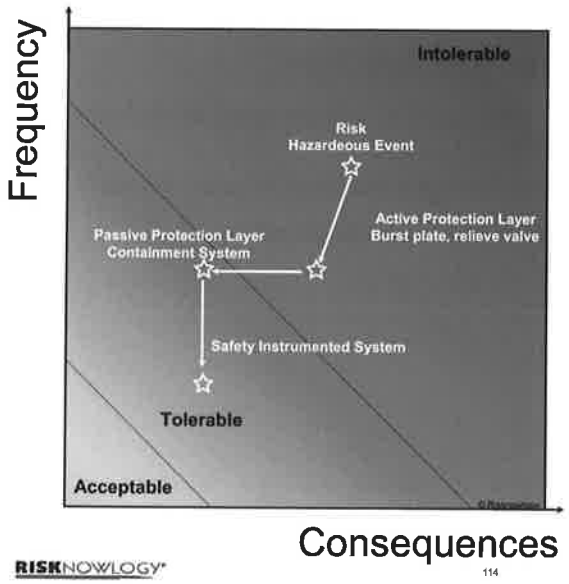


RISKNOWLOGY®

113

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction In Practice



	Consequence	Frequency
Active	X	X
Passive	X	-
SIS	-	X

RISKNOWLOGY®

114

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Management

- Three important steps
  - Identify the hazards / hazardous events
  - Analyze the hazards / hazardous events
  - Reduce risk where necessary
- How do we do that? Three categories of techniques are available
  - Qualitative: everything expressed in words
  - Quantitative: everything expressed in numbers
  - Semi-quantitative: a mixture of words and number

How

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard Identification

- Hazard identification
  - Once all hazards are identified the job is half done
  - Is the first and most important step when identifying the required safety functions for your safety instrumented systems
  - A safety function is useless if it is not linked to a hazard or hazardous event
  - Safety Instrumented Systemss not based on hazards are either
    - Over dimensioned $$$ or
    - Under dimensioned $$$$$$

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard Identification Techniques

- Many hazard identification techniques exist
- Some examples in use today are
  - Check list analysis
  - What if analysis
  - *Failure modes and effects analysis* FMEA
  - *Fault tree analysis* FTA
  - *Hazard and operability analysis* HAZOP
  - ...

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Hazard Identification Techniques

- For all techniques counts that...
  - Best performed in a team (different discipline)
  - Information needed includes:
    - The physical environment of the process including neighbors
    - The equipment under control (EUC)
    - The basic process control system and its functions
    - Information about hazards and basic materials
      (toxicity, explosive conditions, corrosiveness, reactivity, flammability, etc)
    - Existing safety regulations
      (laws, standards, industry guidelines, etc)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Failure Mode and Effects Analysis FMEA

Design, Verification, Qualitative Technique.

- About FMEA
  - First formal applications in 1960 in the aerospace industry
  - It can be used for products, systems and processes
  - First of all it is a design technique
  - But it is better known as a verification technique
  - It is mainly used as a qualitative technique

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Failure Mode and Effects Analysis

One element at a Time

- ...more specifically it
  - Is a bottom-up technique
  - Is a single failure mode analysis technique
  - Does not consider multiple failures at the same time
    - Common cause are not explicitly addressed

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Different Variations Exist

- FMEA can be adjusted to the problem or needs at hand, e.g.:
  - FMEA – Failure mode and effects analysis
    - Basic technique for products and processes
  - FMECA – Failure mode, effects, and criticality analysis
    - For process
  - FMEDA – Failure mode, effects and diagnostic analysis for manufacturer
    - For products
  - Functional FMEA
    - Process is analyzed based on functions rather then the hardware (and software) used to carry out the functions process point of view

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Process FMEA

				Hazard class						
Component	Failure or error mode	Effects on other system components	Effects on whole system	1	2	3	4	Failure frequency	Detection methods	Compensating provisions and remarks
Pressure relief valve	Jammed open	Increased operation of temperature sensing controller and gas flow due to hot water loss	Loss of hot water; greater cold water input, and greater gas consumption	1				Reasonably probable	Observe at pressure relieve	Shut off water supply, reset or replace relief valve
	Jammed close	None	None	1				Probable	Manual testing	Unless combined with other component failure this failure has not consequence
Gas Valve	Jammed open	Burner continuous to operate. Pressure-relief valve opens	Water temperature and pressure increase. Water -> steam			3		Reasonably probable	Water at faucet too hot	Open hot water faucet to relieve pressure. Shut off gas supply. Pressure relief valve compensates
	Jammed close	Burner ceases to operate	System fails to produce hot water	1				Remote	Observe at output	

Source: Recht, Himmelblau, 1978
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Typical Steps

- Typical steps to conduct an FMEA study
  - Define scope of the analysis
  - Define system function to be analyzed
  - List all components
  - Identify failure modes
  - Analyze the effects
  - Document the results
  - Identify any other information of interest
    - Failure rates, causes, independent protection layers, etc

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Another Example of an FMEA Worksheet

Component Information			Failure Information					
Name	ID	Function	Failure mode	Failure rate	Cause	Effect Component Level	Effect System Level	Probability
SOV	SOV 1	Pilot valve for main air supply ESD valve	Stuck open	5.50E-07	Internal mechanical failure	Continous air supply	ESD valve cannot shutdown upon demand	Low
			Stuck close	4.60E-05	Internal mechanical failure	No air flow	ESD valve closes without a demand, spurious trip	Low
			Leakage	1.30E-04	Connection not tight	Limited air supply	ESD valve closes without a demand, spurious trip	Very low

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Failure Rate

Component Information			Failure Information		
Name	ID	Function	Failure mode	Failure rate	Cause
SOV	SOV1	Pilot valve for main air supply ESD valve	Stuck open	5.50E-07	Internal mechanical failure
			Stuck close	4.60E-05	Internal mechanical failure
			Leakage	1.30E-04	Connection not tight

Example Failure Rate Table

Qualitative	Quantitative
Very high	$L > 0.1$
High	$0.01 \leq L < 0.1$
Medium	$0.001 \leq L < 0.01$
Low	$0.0001 \leq L < 0.001$
Very low	$0.00001 \leq L < 0.0001$

RISKNOWLOGY®

125

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Effects

Failure Information					
Failure mode	Failure rate	Cause	Effect Component Level	Effect System Level	Probability

Example Effect Table

Failure effect	Description
Personal or environmental damage	The failure will have severe effect on people and environment
System damage	The failure will damage or destroy the system
Less reliability / availability	The failure will sometimes lead to degraded performance of the system
Disturbing	The failure will lead to failures on function level of this component
Almost no effect	The failure will not have much influence on the performance of the system

Example Probability Table

Qualitative	Quantitative
Sure	$0.95 \leq p < 1$
Probably	$0.5 \leq p < 0.95$
Likely	$0.05 \leq p < 0.5$
Unlikely	$0 \leq p < 0.05$

Probability that the effect actually takes place

RISKNOWLOGY®

126

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

FMEA Results

- Advantages of FMEA
  - You have a complete documented safety study
  - Easy to understand and to apply
  - Easy to verify
- Disadvantages of FMEA
  - Can be a lot of work for an existing process
  - Does not consider multiple failures at the same time (common cause)
  - Only good results if all details are available

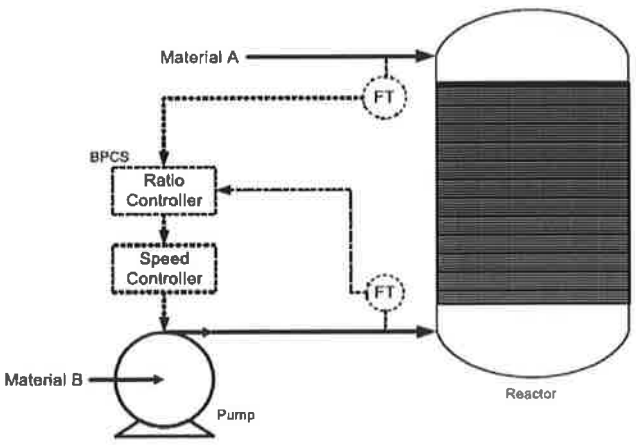
RISKNOWLOGY®

127

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise #04

- Case Study: Carry out an FMEA



RISKNOWLOGY®

128

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Fault Tree Analysis

- About FTA
  - It is a top down technique
  - It starts with an undesired top event and from there we try to find out all possible combinations of failures that can lead to the top event
  - It is a verification technique
  - Can be performed qualitative as well as quantitative
  - Most common technique for causal analysis in risk and reliability studies, specially in the nuclear industry

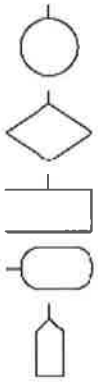
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Typical Steps

- Typical steps to conduct an FTA study
  - Define scope of project
  - Select a set of symbols
    - Depends on software tool
  - Define the top event
  - Create fault tree
  - Analyze the fault tree
  - Document results

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Typical FTA Event Symbols



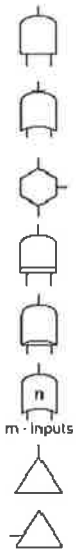
Primary or base event	Bas c fault event requiring nc further development
Undeveloped event	Fault evert which has not been further developed
Intermeciate event	Fault evert which occurs due to antecedent causes acting through a logic gate
Conditioning event	Specific condition which applies to a logic gate (used mainly with Priority, And, and Inhibit gates)
External event	External even which is normally expected to occur

Source: IEC 61025

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Typical FTA Logic Symbols



AND gate	Output exists only if all inputs exist
OR gate	Output exists if one or more inputs exist
INHIBIT gate	Output exists if input occurs in presence of the specific enabling condition (specified by conditioning event to right of gate)
PRIORITY AND gate	Output exists if all inputs occur in a specific sequence (specified by conditioning event to right of gate)
EXCLUSIVE OR gate	Output exists if one and only one input exists
VOTING gate	Output exists if there are m-out-of-n inputs
TRANSFER IN	Symbol indicates that the tree is developed further at the corresponding TRANSFER OUT symbol
TRANSFER OUT	Symbol indicating that the portion of the tree below the symbol is to be attached to the main tree at the corresponding TRANSFER OUT symbol

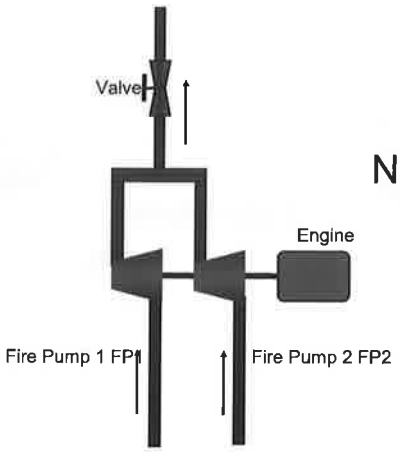
Source: IEC 61025

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

FTA Example Fire Pumps

- Redundant fire pumps

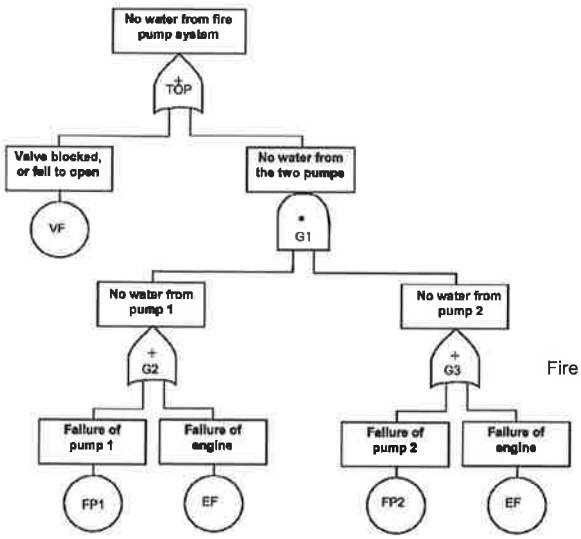


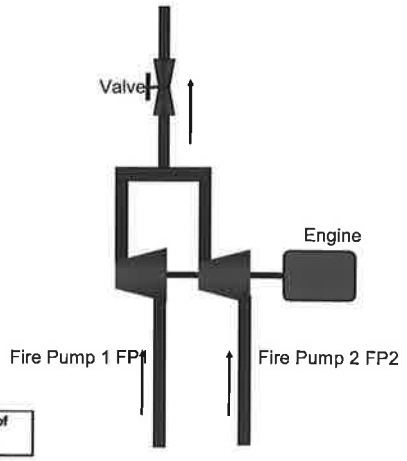
TOP event:
No water from fire water system

Source: Karydas, 2005

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

FTA Example Fire Pumps

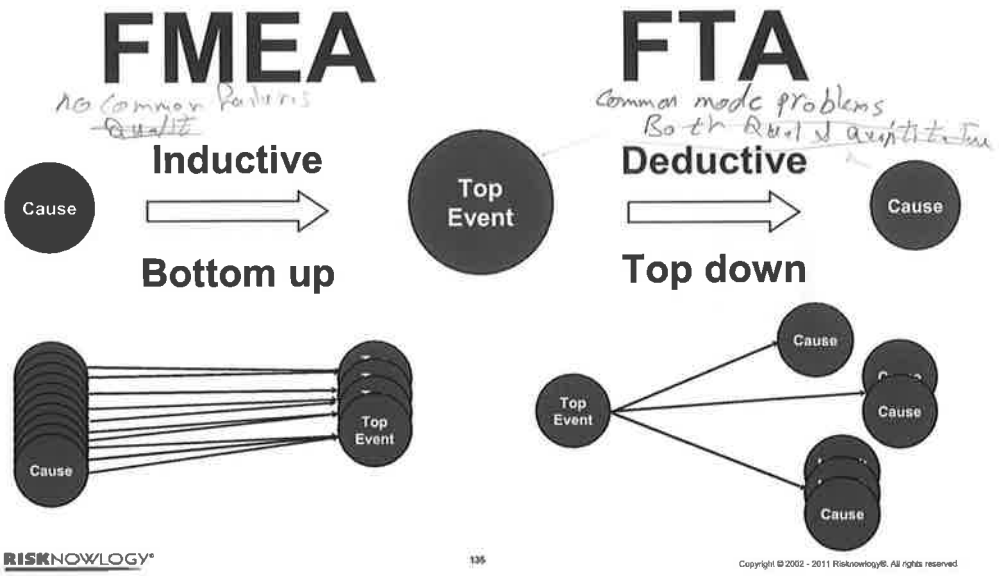




Source: Karydas, 2005

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

FMEA – FTA Relationship



RISKNOWLOGY®

135

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

FTA Results

- Advantages of FTA
  - You found all possible combinations of equipment failures that can lead to a problem
    - You can find common mode problems
  - You can calculate the probability of the top event occurring

RISKNOWLOGY®

136

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

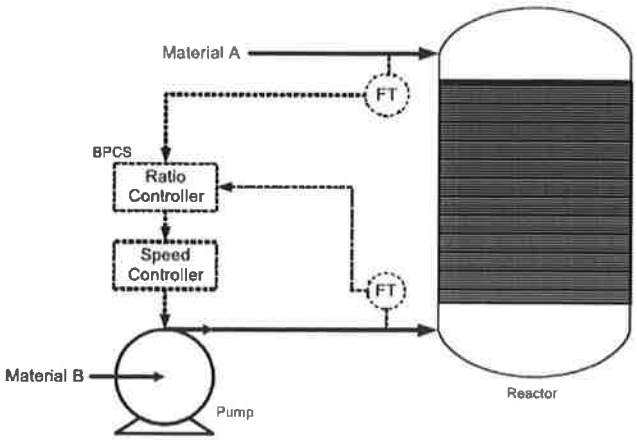
Disadvantages FTA

- Disadvantages are
  - If you do not know what the TOP event should be then you will never create a fault tree for it
  - Each TOP event needs a new fault tree a lot of Trees
  - Associated with the nuclear power industry, it has a "it does not apply to our industry" reputation
  - Only good results if all details are available
  - Difficult to verify a fault tree

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise #05

- Case Study: Carry out an FTA



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 06

- An accident animation is shown
  - Document what goes wrong
  - And how it could have been prevented
- Lets take a look at what happened

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Hazard and Operability Study

- About HAZOP in(Process) not in equipment
  - Popular technique in the process industry
  - Identifies hazards and operability problems
  - Mainly qualitative
  - Very systematic technique
  - Can be used
    - During initial design of a plant
    - During modifications and periodic reviews of existing processes
    - For continuous and batch processes

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Is HAZOP?

- A HAZOP
  - Is a structured and critical examination of a process
    - Not of equipment
  - All possible deviations from the design intent are examined
  - The consequences of the undesirable effects are examined

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Typical Steps

- Typical steps to conduct an HAZOP study
  - Define scope of project
  - Determine guide words
  - Determine study nodes
  - For each node determine the design intent
  - Apply guide words to each study node
  - Document results

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Guide Words

Guide word	Meaning
No (not, none)	None of the design intent is achieved
More (more of, higher)	Quantitative increase in a parameter
Less (less of, lower)	Quantitative decrease of a parameter
As well as (more than)	An additional activity occurs
Part of	Only some of the design intent is achieved
Reverse	Logical opposite of the design intention occurs
Other than (other)	Complete substitution
Other useful Guide Words	
Where else	Applicable for flows, transfers, sources and destinations
Before/after	The step is out of sequence
Early/late	The timing is different
Faster/slower	The step is done/not done with the right timing

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Parameters and Deviations

- The guide words are useless without a parameter
- Typical parameters are:
  - Temperature
  - Pressure
  - Flow
  - Reactants
  - Phase
  - Etc
- Guide word + parameter = deviation

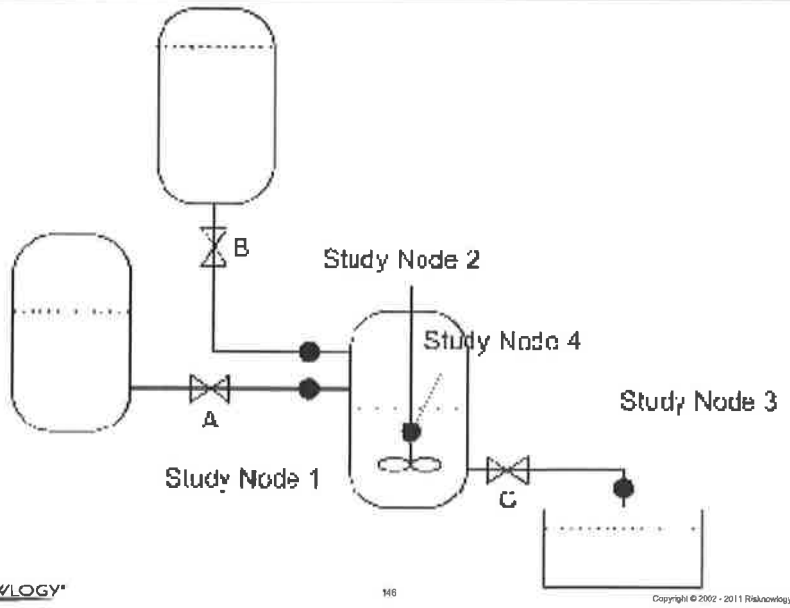
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Examples Process Deviations

Guide Word	Parameter	Deviation
NO	Flow	No flow
MORE	Pressure	High pressure
AS WELL AS	One phase	Two phase
OTHER THAN	Operation	Maintenance

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Choosing Study Nodes



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Operating Deviations

- HAZOP can be applied to operating instructions
- For example:
  - Operator should start flow A thirty seconds after temperature B is reached
- Guide words are applied to
  - Flow A: No, More, Less, etc
  - Flow A: Faster, slower
  - Temperature B: Higher, lower
  - Temperature B: Sooner, later

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example HAZOP Sheet

NODE: Feed section from intermediate storage to buffer/settling tank				
Guide Word	Deviation	Possible Causes	Consequences	Action required
NONE	No Flow	(1) No hydrocarbon available at intermediate storage	Loss of feed to reaction section and reduced output. Polymer formed in heat exchanger under no flow conditions	(a) Ensure good communications with intermediate storage operator (b) Install low level alarm on settling tank LIC
		(2) J1 pump fails	As for (1) As for (1), J1 pump overheats	Covered by (b) Covered by (b) (c) Install kick-back on J1 pumps
		(3) Line blockage, isolation closed in error, or LCV fails shut		(d) Check design of J1 pump strainers Covered by (b)
		(4) Line Fracture	As for (1) Hydrocarbon discharge into area adjacent to public highway	(e) Institute regular patrolling and inspection of transfer line
MORE OF	More flow	(5) LCV fails open or LCV bypass open in error	Settling tank overfills	(f) Install high level alarm on LIC and check sizing relief opposite liquid overfilling (g) Institute locking off procedure for LCV bypass when not in use

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

HAZOP Results

- Advantages of HAZOP are
  - It is a team effort
    - Collectively we should know more
    - All disciplines involved
  - Once finished you have a complete documented safety study
  - Relatively easy to verify

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

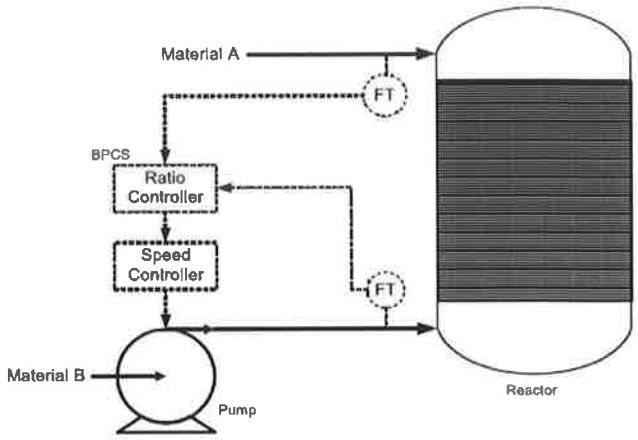
HAZOP Results

- Disadvantages of HAZOP are
  - It is a team effort
    - Team is not creative enough
    - Team does not think in problems but in solutions
    - Too many, too little team members
    - Nodes are not selected correctly
  - Management commitment is necessary - because it is a team effort it involves a lot time and resources
  - It only looks at hazards from inside the process

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise #07

- Case Study: Carry out a HAZOP



identify the hazard
risk analysis
risk reduction

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 08

- Evaluation
  - What are the main differences between the three techniques?
  - Which technique was the best? actually there is no the best but depend on what you are looking for
  - When would you apply which technique? for

process → HAZOP
event → FTA
equip → FMEA

FMEA
—
Bottom-up
equipment
*

FTA
—
* Update
* more to give quantitative
* events

HAZOP
systematic
—
* Process

focusing in
Process
equip
event

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard Analysis

- Hazard analysis is the next step after identification
  - Often it is clear what to do once a hazard is identified
  - For some hazards it is not clear what their likelihood and consequences really are
  - Hazard analysis helps understand what the most cost-effective measure is to guard against the hazard

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hazard Analysis Techniques

- Hazard analysis techniques in use today
  - Fault tree analysis
  - Event tree analysis
  - Cause consequence diagrams
  - Dispersion modeling
  - ...

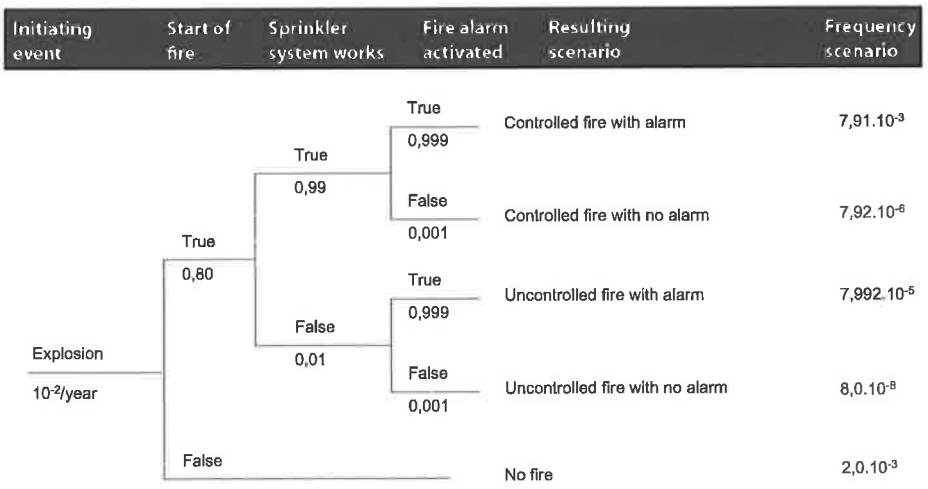
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Event Tree Analysis

- About ETA
  - Helps us understand the consequences of events
  - Models an initiating event and the time sequence of event propagation to the potential consequences
  - Can be used qualitatively as well as quantitatively
  - Can be developed independently or in combination with fault tree analysis

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

ETA Example



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction

- At this point we know
  - Our hazards
  - The consequences of the hazards
  - The likelihood or frequency of the hazards
- Now we need to ask ourselves
  - Do we need to reduce the risk?
  - By how much do we need to reduce the risk?
  - Is a safety instrumented system necessary?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction Analysis Techniques

- Risk reduction analysis techniques in use today
  - Risk matrix
  - Risk graph
  - FMEA
  - Fault tree analysis
  - HAZOP
  - Event tree analysis
  - Layer of protection analysis (LOPA)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction With FMEA And Risk Matrix

Failure Information					
Failure mode	Failure rate	Cause	Effect Component Level	Effect System Level	Probability

Example Risk Reduction Table

Failure Effect	Very Unlikely	Likely	Probably	Sure
	0 - 0.05	0.05 - 0.5	0.5 - 0.95	0.95 - 1
Personal or environmental damage	SIL 3	SIL 4	SIL 4	Unacceptable
System damage	SIL 2	SIL 3	SIL 4	SIL 4
Less reliability / availability	SIL 1	SIL 2	SIL 3	SIL 4
Disturbing	-	SIL 1	SIL 2	SIL 3
Almost no effect	-	-	SIL 1	SIL 2

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Risk Reduction With HAZOP

NODE: Dilution air inlet line to suction of oxidizer blower							
Deviation	Cause	Consequence	Safeguards	C	F	SIL	Recommendation
Low Flow	Valve FCV-1 not fully open	Increase VOC in gas stream Potential explosion if VOC>LEL and gas reaches incinerator	LEL SENSOR causes diversion of gas stream to atmosphere by opening valve FCV-2A and closing the oxidizer blocking valve CV-2B Pressure relieving panels Detonation arrestor	3	2	2	Check response time of LEL sensor Provide LIMIT SWITCH on valve Provide LOW FLOW ALARM Verify operator procedures Verify if relief area is adequate

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Consequences

Consequence Range	Qualitative Criteria
4	**Personnel:** Multiple critical injuries or fatalities **Public:** Potential for multiple critical injuries or fatalities **Environment:** Unconfined release with major environmental impact **Property:** Plant & production loss in excess of $100 M
3	Personnel: Potential for serious injuries or single fatality Public: Potential for serious injuries or single fatality Environment: Unconfined release with medium environmental impact Property: Plant & production loss in the range of $10 to $100 M
2	Personnel: severe injury requiring medical emergency care Public: Potential for severe injury requiring medical emergency care Environment: Unconfined release with minor environmental impact Property: Plant & production loss in the range of $1 to $10 M
1	Personnel: Injury requiring first aid Public: Odor or noise nuisance, no direct impact Environment: Confined release with localized impact Property: Plant & production loss in the range of $0 to $1 M

RISKNOWLOGY®

161

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Frequency

Frequency Range	Quantitative (by numbers) Criteria
4	(greater than 1/100 yr.) e.g., single instrument or valve failure, hose failure or a single error in routine activity
3	(1/100-1/1000 yr.) e.g., dual instrument or valve failure, hose rupture, piping leak, or human error
2	(1/1000-1/10,000 yr.) e.g., combination of instrument failures and human errors, or guillotine breaks of small process lines or fittings.
1	(less than 1/10,000 yr.) e.g., multiple instrument or valve failures or human errors, or spontaneous failures of tanks or process vessels.

RISKNOWLOGY®

162

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Frequency

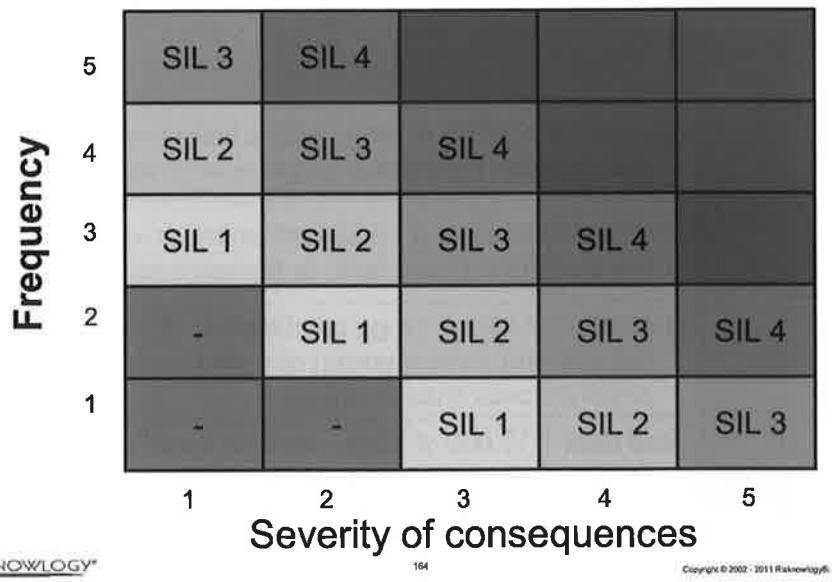
Frequency Range	Qualitative (by words) Criteria
4	Very high, e.g., single instrument or valve failure, hose failure or a single error in routine activity
3	High, e.g., dual instrument or valve failure, hose rapture, piping leak, or human error
2	Low, e.g., combination of instrument failures and human errors, or guillotine breaks of small process lines or fittings.
1	Very low, e.g., multiple instrument or valve failures or human errors, or spontaneous failures of tanks or process vessels.

RISKNOWLOGY®

163

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Reduction Matrix

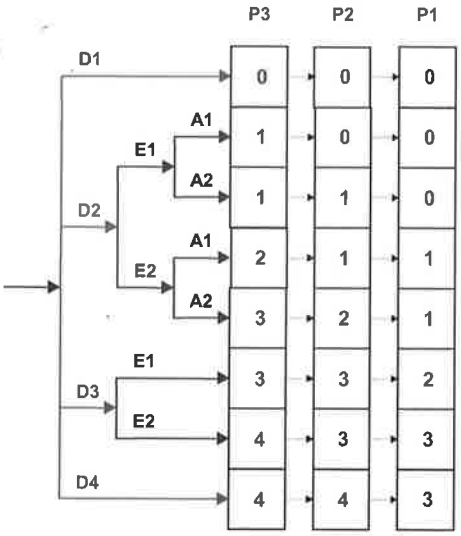


RISKNOWLOGY®

164

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Risk Graph Example



Risk Parameters

D - Extent of Damage

- D1: slight injury
- D2: severe irreversible injury to one or more persons or death of a person
- D3: Death of several persons
- D4: Catastrophic consequences, multiple deaths

E - Exposure Time

- E1: seldom to relatively frequent
- E2: frequent to continuous

A - Hazard Avoidance / Mitigation

- A1: possible under certain conditions
- A2: hardly possible

P - Occurrence Probability

- P1: very low probability
- P2: low probability
- P3: relatively high probability

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved

Risk Graph (UKOOA)

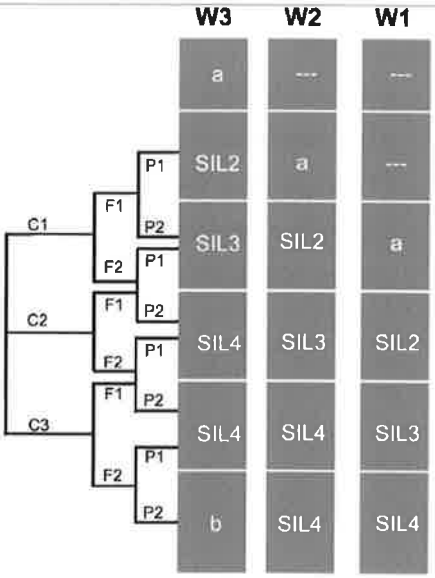
C1 Replacement cost less than $5
C2 Replacement cost more than $5M, less than $50M
C3 Replacement cost more than $50M

F1 Production rate up to 10,000 bbls/day
F2 Production rate more than 10,000 bbls/day

P1 Possible for operator to take action to prevent incident or to significantly reduce consequences
P2 Unlikely that operator action will prevent or mitigate consequences

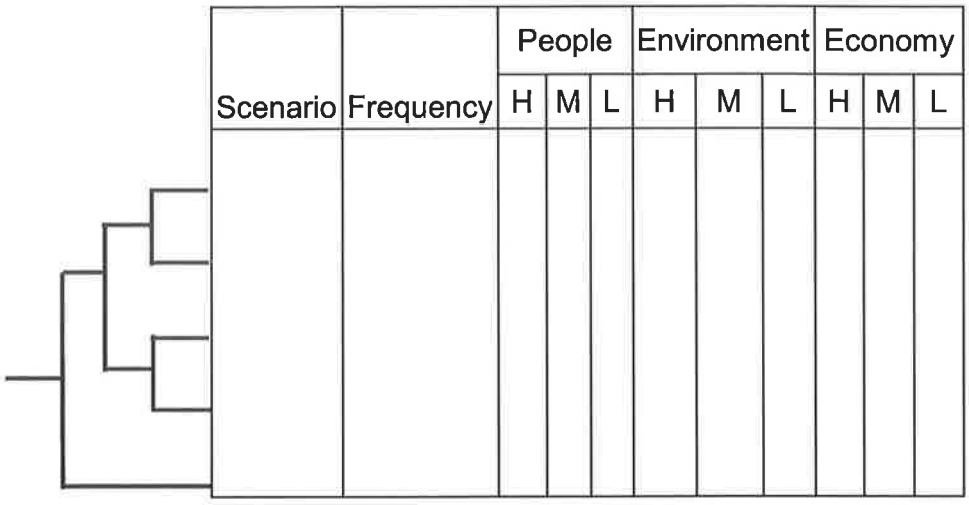
W1 Demand occurs very rarely
W2 Demands occur on an average basis
W3 Frequent demands

--- No safety requirements
a No special safety requirements
b An E/E/PES is not sufficient



Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved

ETA Example



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Layer of Protection Analysis

Risk reduction

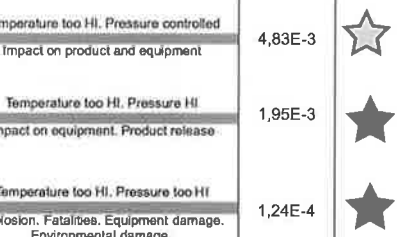
Using event Tree

- About LOPA
  - It helps determine the frequency of occurrence of the hazardous event
  - It is a modified version of event tree analysis
  - It helps establish the frequency of a hazardous event leading to an accident
  - It takes into account only protection layers
  - Can be used qualitatively as well as quantitatively

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

LOPA Example

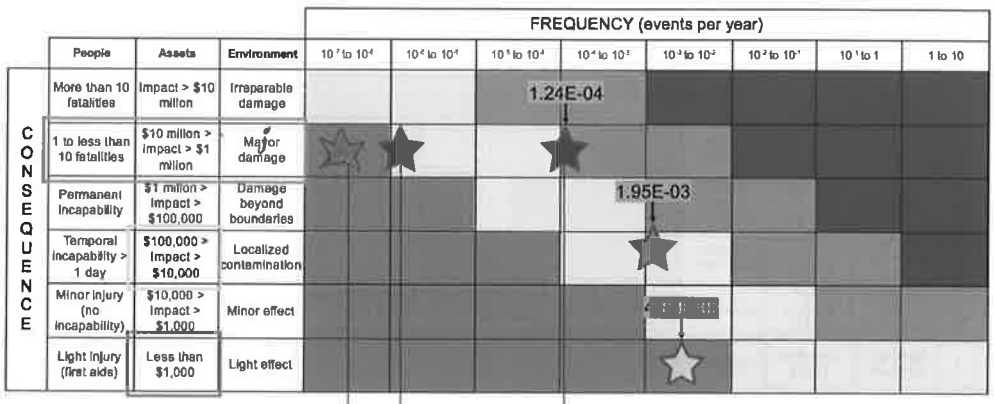
Exothermic Reaction	Temperature Control	Pressure Control	Relief Valve	Outcome / Consequence	Frequency
	7,0E-1			Temperature Controlled. Pressure normal	1,61E-2
				Impact on product quality	
2,30E-2		7,0E-1		Temperature too HI. Pressure controlled	4,83E-3
(times/year)				Impact on product and equipment	
	3,0E-1		9,40E-1	Temperature too HI. Pressure HI	1,95E-3
	(PFD)			Impact on equipment. Product release	
		3,0E-1			
		(PFD)			
			6,0E-2	Temperature too HI. Pressure too HI	1,24E-4
			(PFD)	Explosion. Fatalities. Equipment damage. Environmental damage.	



RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

LOPA Example



$$RRF = \frac{\text{Event Frequency}}{\text{Tolerable Frequency}}$$

PFD = 1/ RRF

RRF = 100 (SIL 2)

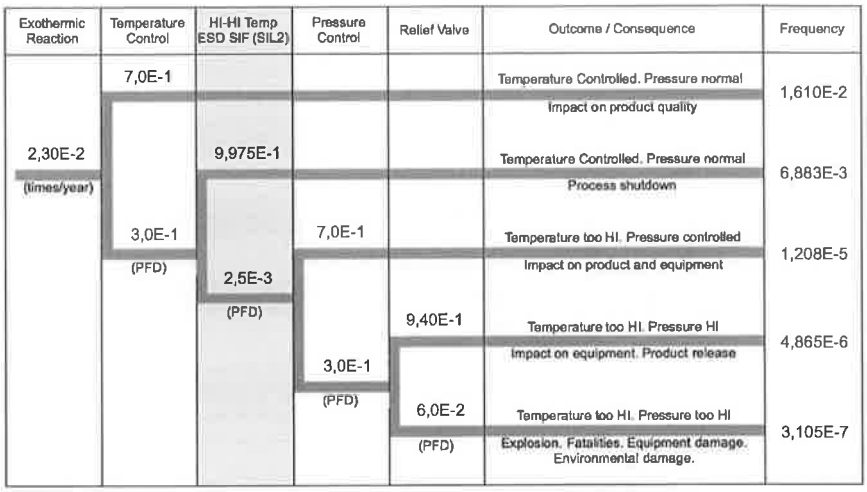
RRF = 400 (SIL 2)

Defining just SIL 2 is not enough!
Which PFD do we need?

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

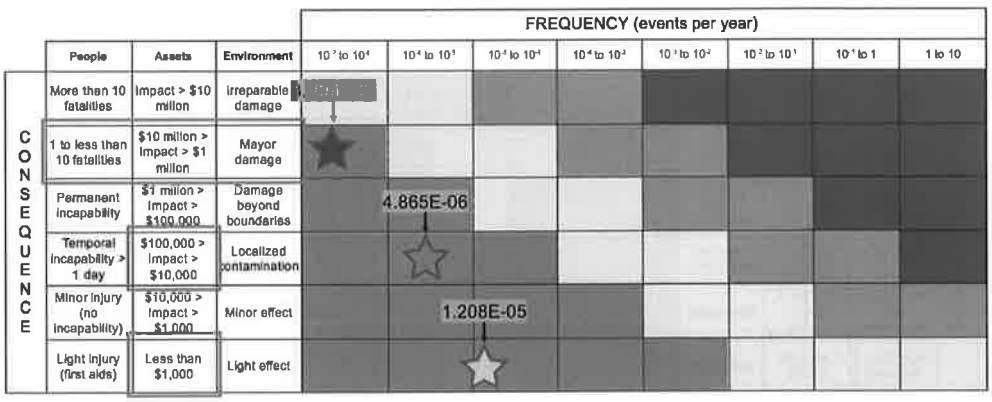
LOPA Example



Adding a SIL 2 SIF with PFD = 2.5E-03

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

LOPA Example



A SIL 2 SIF with PFD = 2.5E-03 will do the job

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

LOPA Results

- Advantages
  - More accurate modeling compared to Risk Graph or Risk Matrix
  - Takes into account unlimited numbers of available protection layers
- Disadvantages
  - LOPA is suitable for playing with numbers
  - Often credit is given for wrong or non-protection layers
    - Pay attention to common cause between layers
    - Pay attention to what actually a protection layer is and what is not

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

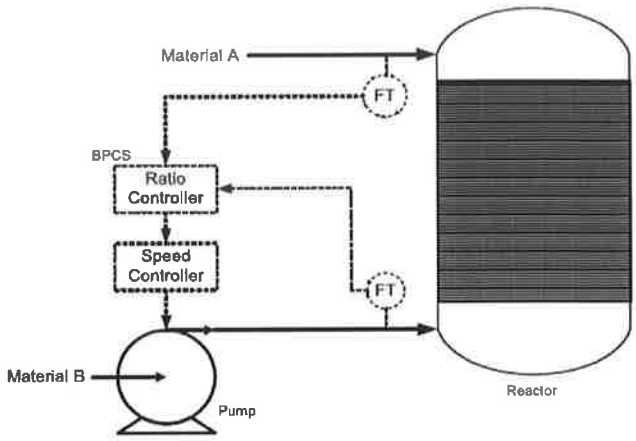
Pay Attention!

- For all techniques/tools counts
  - They are only as good as you use them
  - Garbage in means garbage out
  - Any technique based on data requires reliable data to get reliable results
- Create company procedures for each technique you want to use
  - What are the rules of the technique?
  - When to apply which technique?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise #09

- Case Study: Select the appropriate SIL



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Function

- There are five basic properties
  - Sense
  - Logic
  - Actuate
  - Timing response Time of the SF
  - Safety integrity (SIL)
- Timing is determined by the process safety time
  - Rule of thumb: Timing ≤ Process Safety Time / 2

environment of
if configuration too big + means SIS will Take Time to execute the required action & also if process is too fast, then Time is important

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Environment of condition also should to be considered here

Bad Example of a Safety Function

- From practice:
  - "The main safety function of the HIPPS is to protect the separation vessels against overpressure and to protect the low pressure equipment against high pressure."

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Better Example of a Safety Function

- Example of a safety function
  - "Measure the temperature in vessel V23 in two locations and if the temperature exceeds the 65 ℃ temperature limit open the drain valve within 3 seconds. The safety integrity of this safety function should meet SIL 3."

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Requirement Specification

- The end-users SRS could include things like:
  - Functional description of all safety functions
  - Safety integrity level
  - Required Risk Reduction Factor
  - Energize to trip or de-energize to trip
  - Low demand, high demand or continuous mode
  - Safe state for each safety function
  - Startup, restart, reset functionality
  - Maximum allowable spurious trip level (STL)
  - Environmental conditions (Temperature, EMC, humidity, vibration, etc.)
  - Bypass philosophy / override
  - Etc

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Summary Module 3

- In this module we addressed
  - How to identify hazards
  - How to analyze hazards
  - That frequency x consequence = risk
  - How to determine risk reduction
  - That a risk matrix or graph can help us determine the SIL per safety function
  - That once the safety function is defined we can write a top level SRS

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Do the job correctly as per planning

Planning The Safety Instrumented System

RISKNOWLOGY®

181

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Planning the Safety Instrumented System

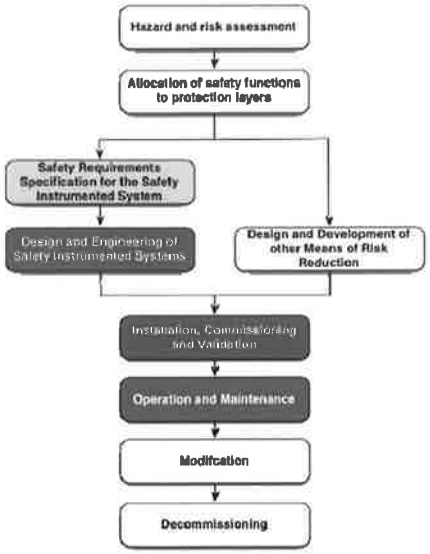
- In this module
  - Overall planning
  - Implementation of a safety instrumented systems
  - Safety plan, V&V plan and overall SRS
  - Requirements for suppliers

RISKNOWLOGY®

182

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Where Are We?


Hazard and risk assessment
Allocation of safety functions to protection layers
Safety Requirements Specification for the Safety Instrumented System
Design and Engineering of Safety Instrumented Systems
Design and Development of other Means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Planning for End Users (Integrators)

- What needs to be planned
  - Overall installation and commissioning
  - Overall safety validation
  - Operation and maintenance

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

End Users Need

- At this point the end user
  - Knows which safety functions there are
  - Knows which safety functions will be implemented in which technology
  - Needs sufficient information (documentation) from his suppliers to plan his activities

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Typical Questions

- An end-user should understand what to expect
  - Do we need to train our personnel?
  - Do we need to hire new people with special expertise?
  - Do we need to buy special tools or equipment?
  - Do we need to change or create new procedures?
  - Etc
- Do we have proper functional safety management in place?
  - Do we have a functional safety manager?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Realization Safety Instrumented System

- Realization is done by
  - Integrators and/or product manufacturers
- What do integrators and products manufacturers deliver?
  - Hardware and/or
  - Software
  - Documentation
    - Including documentation to operate, maintain, validate, commission and install the safety instrumented systems

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Three Important Documents

- When we start with the physical safety instrumented systems the following three documents are important
  1. Safety plan
  2. Verification & validation plan
  3. Safety requirements specification
- The user, the integrator, the manufacturer, they all have their own versions of these documents
- The functional safety manager(s) needs to manage these documents

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Plan

- Objective
  - How do we plan to achieve functional safety?
- Typical content
  - Lifecycle(s) and phases
  - People, organizations and responsibilities
  - Tools, techniques, etc
  - Modification procedure

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Verification & Validation Plan

- Objective
  - Did we build the safety instrumented systems right? - Verification
  - Did we build the right safety instrumented systems? - Validation
- Typical content
  - Who verifies/validates what?
  - When verification/validation is done?
  - How verification/validation is done?
  - Which tools, techniques, knowledge are needed?
  - Etc

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Requirements Specification

- The end-user knows his specification as it resulted from the hazard and risk analysis
- Often system integrators build the actual safety instrumented systems and their safety functions
- Recommendation
  - Translate the end-user safety requirements specification into a system integrator safety requirements specification
    - Hardware requirements
    - Software requirements
  - Have the end-user approve the system integrator safety requirements specification before the design and engineering work starts

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Requirements For Suppliers

- Suppliers of safety equipment should make sure that end-users get enough information so that they can easily
  - Operate and maintain
  - Validate
  - Commission and install
  - And prove that their safety functions are compliant
- Usual this is done via product manuals
- But also system integrators need to think about manuals on system level

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Summary Module 4

- In this module we addressed
  - What needs to be planned
  - What an end user needs to know
  - The realization of the safety instrumented systems
  - The three most important documents in the safety industry
  - Requirements for suppliers
  - Need for a functional safety manager

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hardware Design

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hardware Design

- In this module
  - Hardware lifecycle
  - Hardware concepts
  - Architectural constraints
  - Measures to control and avoid failures
  - Reliability analysis

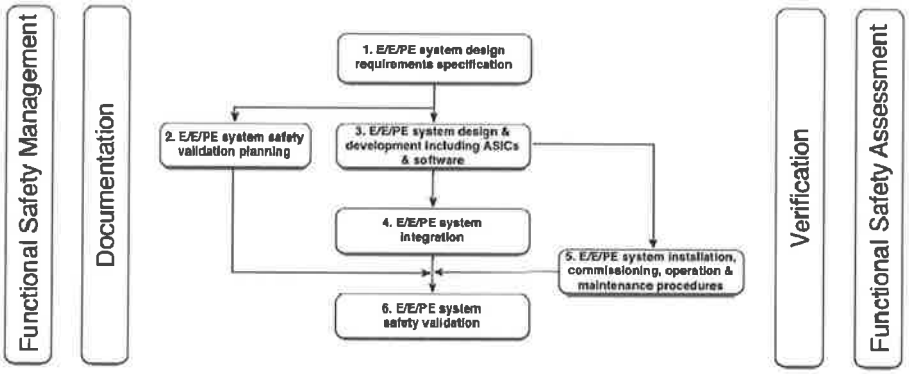
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Where Are We?

Hazard and risk assessment
Allocation of safety functions to protection layers
Safety Requirements Specification for the Safety Instrumented System
Design and Engineering of Safety Instrumented Systems
Design and Development of other Means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Hardware Lifecycle - IEC 61508


Functional Safety Management
Documentation
1. E/E/PE system design requirements specification
2. E/E/PE system safety validation planning
3. E/E/PE system design & development including ASICs & software
4. E/E/PE system integration
5. E/E/PE system installation, commissioning, operation & maintenance procedures
6. E/E/PE system safety validation
Verification
Functional Safety Assessment

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Fundamental Hardware Concepts

- Hardware design on safety function level
  - De-energize versus energize
  - Low demand, high demand, continuous mode - 61508
  - Demand mode, continuous mode - 61511
  - Target failure measure
    - Probability of Failure Dangerous - PFDavg, PFH
      - A measure for the Safety Integrity Level (SIL)
    - Probability of Fail Safe
      - A measure for the Spurious Trip Level® (STL)

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

De-energize Or Energize To Trip

- What is the difference?
  - A de-energize to trip safety instrumented systems does not need energy to perform its safety function
    - It is based on the so-called fail-safe design principle
  - An energize to trip safety instrumented systems needs energy to perform its safety function
    - This is not fail safe

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

De-energize To Trip Examples

- Fail safe programmable electronic logic solver
  - Safe state is always the 0 state or energyless state
  - Only electrical power will result in a 1 state
- Spring return actuator
  - Energize spring to open valve
  - De-energize spring to close (FC)
  - Fail safe design

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Energize To Trip Examples

- Sprinkler system
  - Pumps
  - Electricity
  - Water
- Fire & gas system
  - Detection and
  - alarm management

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Low Demand, High Demand, Continuous

- IEC 61508 defines 3 types of safety function operations
  - Low demand mode
  - High demand mode
  - Continuous mode

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Low Demand Mode - IEC 61508

- Low demand mode safety function
  - Where the safety function is only performed **on demand**, in order to **transfer** the EUC into a specified **safe state**, and, where the frequency of demands is no greater than **one per year**
- Typical example
  - Emergency shutdown system with ESD valve

RISKNOWLOGY®

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

High Demand Mode - IEC 61508

- High demand mode safety function
  - where the safety function is only performed **on demand**, in order to **transfer** the EUC into a specified **safe state**, and where the frequency of demands is **greater than one per year**;
- Typical example
  - Emergency shutdown system based on drain valve of a batch reactor process

RISKNOWLOGY®

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Continuous Mode - IEC 61508

- Continuous mode safety function
  - where the safety function **retains** the EUC in a **safe state** as part of normal operation.
- Typical example
  - Keep supply valve of gas burner at 50% capacity during start-up procedure

- normal state is the safe state
- immediatly the process will be not available.
- all the time SF retain EUC in safe state as part of normal operation

RISKNOWLOGY

205

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Demand Versus Continuous - IEC 61511

- IEC 61511 defines demand mode and continuous mode
- Demand mode
  - A dangerous failure of the safety function itself has no immediate effect on the process
  - The process is in danger if
    - The safety function has failed dangerous AND
    - A demand occurs
- Continuous mode
  - A dangerous failure of the safety function itself has an immediate effect on the process
  - The process is in danger because the safety function has failed dangerous

RISKNOWLOGY

206

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Pay Attention!

- Each demand needs to be analyzed for its reason(s)
  - Bad process control often results in too many demands
- Frequent demands for a low demand process should not necessarily result in "we need a high demand safety instrumented systems"
  - It might result in changes in process design, operation of the process, procedures, ...

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Probability Of Failure

- For each safety function we need to know how often it fails
- Probability of Failure on Demand - PFD
  - The probability that the safety function does not work upon demand from the process
  - Requirement in IEC 61511
- Probability of Fail Safe - PFS
  - The probability that the safety function is carried out without a demand from the process
  - Not a requirements in IEC 61511

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

PFDavg Versus PFH

- The probability of failure on demand after one year or after one hour

SIL	PFDavg (low) demand mode	PFH high demand / continuos mode
4	$\varepsilon 10^{-5}$ to $<10^{-4}$	$\varepsilon 10^{-9}$ to $<10^{-8}$
3	$\varepsilon 10^{-4}$ to $<10^{-3}$	$\varepsilon 10^{-8}$ to $<10^{-7}$
2	$\varepsilon 10^{-3}$ to $<10^{-2}$	$\varepsilon 10^{-7}$ to $<10^{-6}$
1	$\varepsilon 10^{-2}$ to $<10^{-1}$	$\varepsilon 10^{-6}$ to $<10^{-5}$

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Spurious Trip Level®

- Probability of fail safe - PFS

STL	PFSavg Low demand	PFSh High demand, continuous demand
X	$\varepsilon 10^{-(X+1)}$ to $<10^{-X}$	$\varepsilon 10^{-(X+5)}$ to $<10^{-(X+4)}$
...	...	...
4	$\varepsilon 10^{-5}$ to $<10^{-4}$	$\varepsilon 10^{-9}$ to $<10^{-8}$
3	$\varepsilon 10^{-4}$ to $<10^{-3}$	$\varepsilon 10^{-8}$ to $<10^{-7}$
2	$\varepsilon 10^{-3}$ to $<10^{-2}$	$\varepsilon 10^{-7}$ to $<10^{-6}$
1	$\varepsilon 10^{-2}$ to $<10^{-1}$	$\varepsilon 10^{-6}$ to $<10^{-5}$

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

How To Use the Spurious Trip Level®

- For each safety function estimate how much it costs to have a spurious trip
- The higher the cost the higher the STL should be
- For each company the levels need to be determined individually, see example below

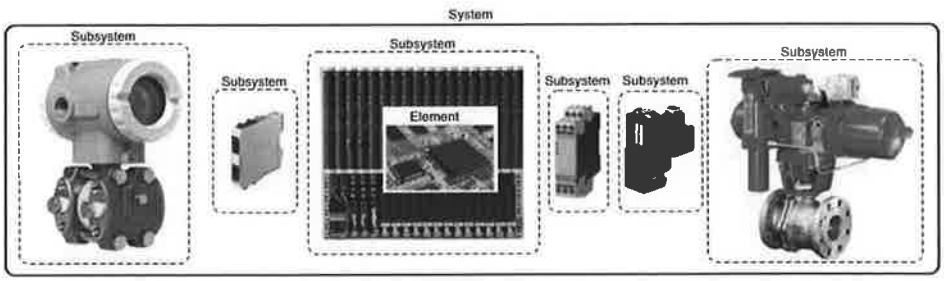
STL[tm]	Cost of a spurious trip due to safety instrumented function
6	Over €20M
5	Between €10M and €20M
4	Between €5M and €10M
3	Between €1M and €5M
2	Between €500k and €1M
1	Between €100k and €500k
None	Between €0 and €100k

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Subsystems

- A safety function is part of system which can have several subsystems and elements
- Any subsystem / element used in the safety function must be a compliant item, i.e., an item that fulfills the requirements of the standard

every element should be of the same SIL



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Fundamental Hardware Concepts

- Hardware design on subsystem level
  - Redundancy and diversity
  - Voting and hardware fault tolerance
  - Type A and Type B
  - Failure modes
  - Detected and revealed failures
  - Safe failure fraction
  - Architectural constraints

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

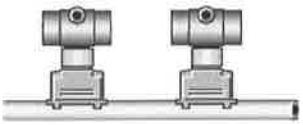
Redundancy

- What is redundancy?
  - Definition
    - The use of the same means to achieve the **same** (or part of the same) safety function
  - Redundancy may be achieved by
    - Same hardware and/or software, or
    - Diverse hardware and/or software
  - Redundancy does not necessarily help against hardware common cause failures and does not help against systematic failures

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Examples – Redundancy

- Redundant equipment



- Diversity is one measure against common cause and systematic failures, but does not necessarily help against all common cause and systematic failures

Copyright © 2002 - 2011 Riskknowlogy®, All rights reserved.

Diversity

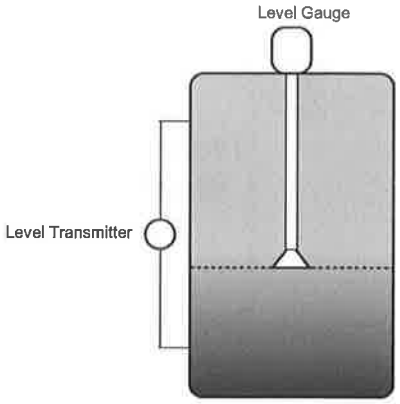
- What is diversity?
  - Definition
    - The use of **different** means to perform the **same** (or part of the same) safety function
  - Diversity can be achieved by
    - Different physical methods
    - Different design philosophies
  - Diversity is one measure against common cause and systematic failures, but does not necessarily help against all common cause and systematic failures

Copyright © 2002 - 2011 Riskknowlogy®, All rights reserved.

Examples – Redundancy

- Diverse equipment

- Diverse design solution



RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Voting

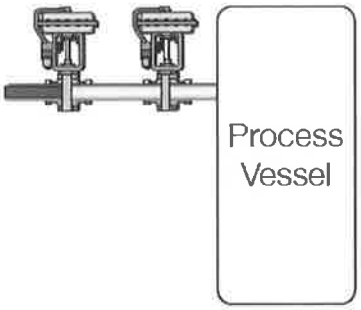
- Voting is defined as
  - The number of independent paths (M) required out of the total number of existing paths (N) in order to perform the safety function
- Voting is often expressed as MooN
  - M expresses the number of voting
  - N expresses the number of redundancy
  - For example 1oo2, 2oo3, 2oo4, etc.
  - Voting can "destroy" redundancy, e.g., 2oo2

RISKNOWLOGY®

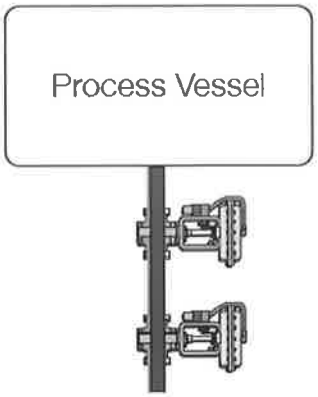
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Examples – Redundancy

- 1oo2 Fail to Close (FC) valves



- 2oo2 Fail to Open (FO) valves



Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Hardware Fault Tolerance (HFT)

- A hardware fault tolerance of N means
  - That N + 1 faults could cause a loss of the safety function
- Hardware fault tolerance is easy to calculate
  - For any MooN system, HFT = N - M
  - For example, the HFT of a 2oo3 system is: 3-2=1

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

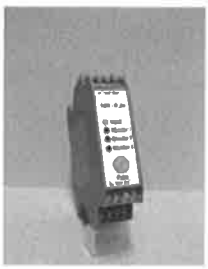
Exercise # 10

Architecture	Voting	Redundancy	HFT
1oo1	no	no	no
2oo2	yes	no	no
1oo2	yes	yess dual red.	1
2oo3	yes	yes triple	1
1oo3	yes	yes Triple red	2
2oo4	yes	Quad	

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Type A Subsystems

- A subsystem is type A if
  - The failure modes are well defined, AND
  - The failure behavior can be completely determined, AND
  - Sufficient failure data is available



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Type B Subsystems

- A subsystem is type B if
  - One or more failure modes are not well defined, OR
  - The failure behavior cannot be completely determined, OR
  - Insufficient failure data is available
- If there is an IC inside you can be 99.9% sure it is a Type B

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Subsystem Failure Modes

- Safe failure
  - The subsystem fails safe, if it carries out the safety function without a demand from the process
- Dangerous failure
  - The subsystem fails dangerous, if it cannot carry out the safety function upon demand from the process
- No effect failure
  - The element that fails is part of the safety function but the failure does not effect that safety function
- No part failure
  - The element that fails is not part of the safety function
- Detected failure
  - A failure is detected if built-in diagnostics reveals the failure

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

How to

Revealing Failures

- Failures can be revealed in three ways:
  - Through normal process operation
  - Through periodic proof tests
  - Through built-in diagnostic tests

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Through Normal Process Operation

- Revealing failures through normal process operations means that
  - The **process behavior** on its own **reveals** the failure of the subsystem, for example
    - The factory shuts down due to a safe failure in the pressure transmitter, or
    - The vessel cannot be emptied due to a dangerous stuck close of the drain valve
- This way of revealing failures is not useful
  - Not from a safety point of view
  - Not from a process availability point of view

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Revealing Through Testing

- In the safety industry a lot of testing takes place
  - Periodic proof tests
  - Built-in diagnostic tests
- Any test features two properties
  - Frequency: How often is it carried out
  - Coverage: The percentage of failures detected
- A test is only useful if we act upon its results and thus a decision is made for further action

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Revealing Failures By Diagnostics

- A test is called a Diagnostic Test when that test
  - Is carried out automatically, AND
  - Is carried out frequently, AND
  - Is used to reveal failures that could jeopardize the safety function, AND
  - Results in an automated safe response
- Usually a diagnostic test is a "built-in" feature
  - For example a memory test, CPU test, watchdog, ...

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

About Diagnostic Frequency

- How frequent should a test be carried out to be called a Diagnostic Test?
  - At least a magnitude (factor 10) faster than the expected demand rate
    - Diagnostic Test Frequency > 10 x Demand Rate
  - For example
    - If the expected demand is once per year, and automatically partial strokes are performed, on a 1oo2 valve configuration, more often than once per month, then that partial stroke test is designed as a Diagnostic Test
      - Provided that 1 valve can always bring the process to the safe state
    - The same automated partial stroke test performed once every 2 months would be designated as a periodic Proof Test

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Revealing Failures By Proof Tests

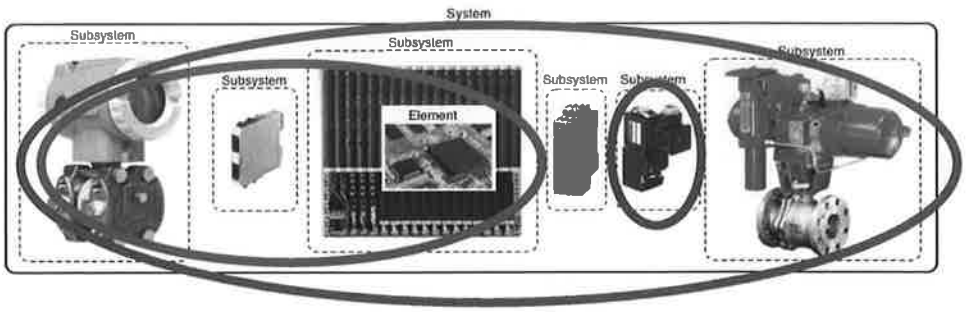
- All other tests are called Proof Tests. They are
  - Not automatic, OR
  - Their frequency is too low
- A proof test is
  - Initiated by human action
  - Usually not "built-in", additional equipment is necessary to carry out the test
- For example an operator performs a Partial Stroke Test (PST) on a safety valve

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

01853945

Proof Test

- We can carry out a proof test on
  - One individual device
  - On a combination of devices
  - On the complete safety loop



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Practical Question...

- Question
  - What are the three practical differences between a Diagnostic and a Periodic Proof Test?
  - Would you rather buy an expensive piece of equipment with a lot of diagnostics or rather buy a cheaper piece of equipment and perform proof tests?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

In Summary

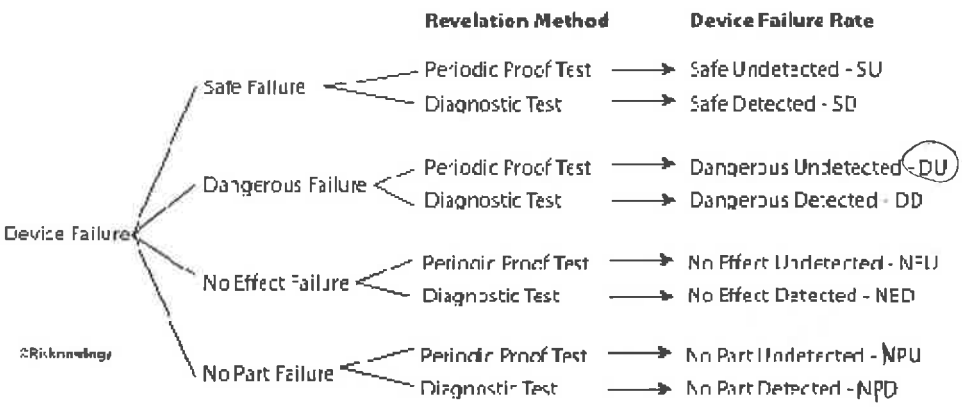
Attribute	Diagnostic Test	Proof Test
Coverage	>0 - ≤100%	>0 - ≤100%
Frequency	High Milliseconds, minutes, hours	Low Days, weeks, months, years
Runs Automatically?	Yes	No
Reacts Automatically?	Yes	No
Build in? (No external equipment needed?)	Yes	No
One Time Startup Cost / Periodic Cost	Yes / No	Yes / Yes

RISKNOWLOGY®

233

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Detected or Not? That Is the Question



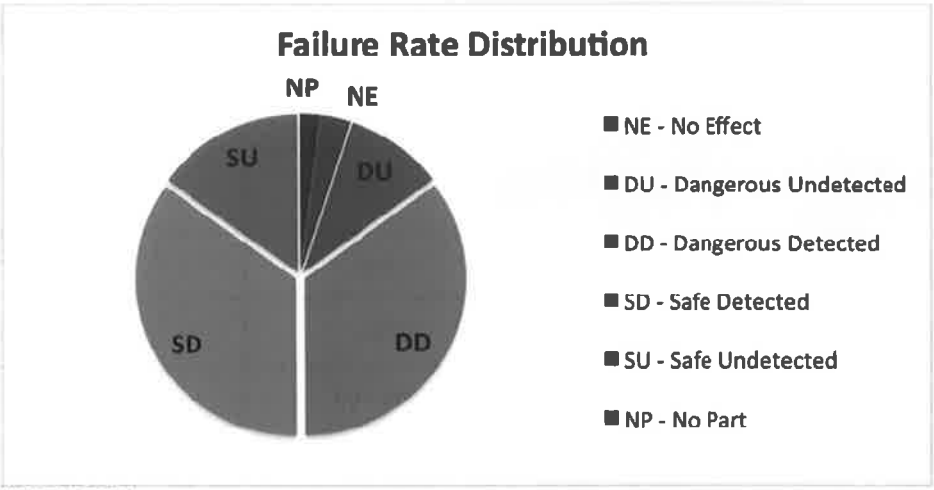
RISKNOWLOGY®

234

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Failure Distribution

- Failure rates are expressed as failures per hour



RISKNOWLOGY®

235

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safe Failure Fraction (SFF)

- What is it?
  - A measure of the effectiveness of the **fail safe** design and/or the **built-in diagnostic tests**
  - It is a design parameter, not an operational parameter
- It is calculated as follows:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}$$

RISKNOWLOGY®

236

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

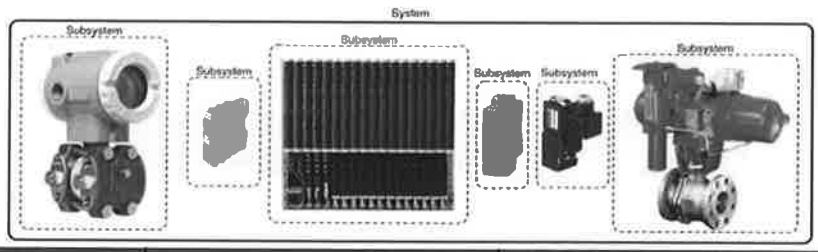
Pay Attention

- A Proof Test cannot be used to calculate the SFF
  - A Proof Test is an operational parameter
- Why does the SFF exist?
  - The PFD reflects how often a subsystem fails in a dangerous undetected mode, this is not enough to express safety
  - The SFF reflects the ratio of dangerous undetected failures inherent in a subsystem
  - Dangerous undetected failures
    - SFF ≈ "How many"
    - PFD ≈ "How often"

Copyright © 2002 - 2011 Riskknowlogy®. All rights reserved.

λ Failure rate

IEC 61508



Safe Failure Fraction (SFF)	Type A Hardware Fault Tolerance (HFT)			Type B Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3	N.A.	SIL 1	SIL 2
60 % - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % - < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Copyright © 2002 - 2011 Riskknowlogy®. All rights reserved.

Architectural Constraints IEC 61511

- Programmable electronic (PE) logic solvers

SIL	Minimum hardware fault tolerance		
	SFF < 60%	SFF 60% to 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply, see IEC 61508		

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Architectural Constraints IEC 61511

- All equipment except PE logic solvers

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	Special requirements apply, see IEC 61508

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

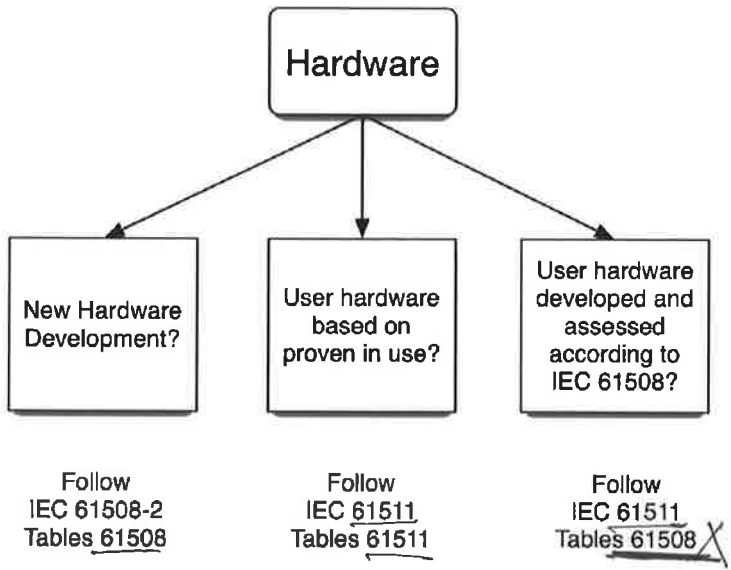
When to reduce or increase HFT?

- You may reduce the HFT by 1 if:
  - The hardware device is selected on prior use, AND
  - Only process related parameters can be adjusted, AND
  - Adjustment of process parameters is protected, AND
  - The SIL is less than 4

- You must increase the HFT by 1 if
  - The dominant failure is not to the safe state, AND
  - Dangerous failures are not detected

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

When IEC 61508 and When IEC 61511?


Hardware
New Hardware Development?
User hardware based on proven in use?
User hardware developed and assessed according to IEC 61508?
Follow IEC 61508-2 Tables 61508
Follow IEC 61511 Tables 61511
Follow IEC 61511 Tables 61508

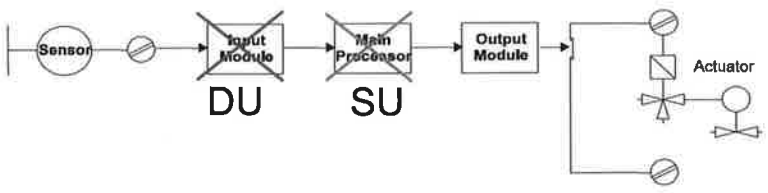
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Architectural Constraints Not Met?

- Real "show stopper"
  - No need to continue
  - No need to make a probability calculation
- What you need to do is
  - **Redesign** the architecture, or
  - **Change** the configuration of the architecture
    - Select more suitable devices
    - Select devices with a higher safe failure fraction

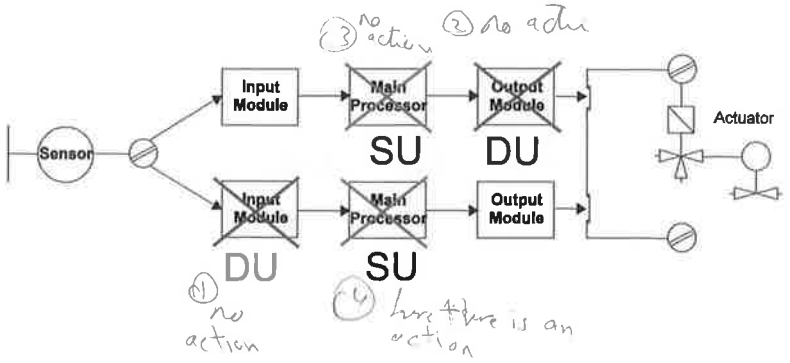
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

1oo1 Safety Instrumented System



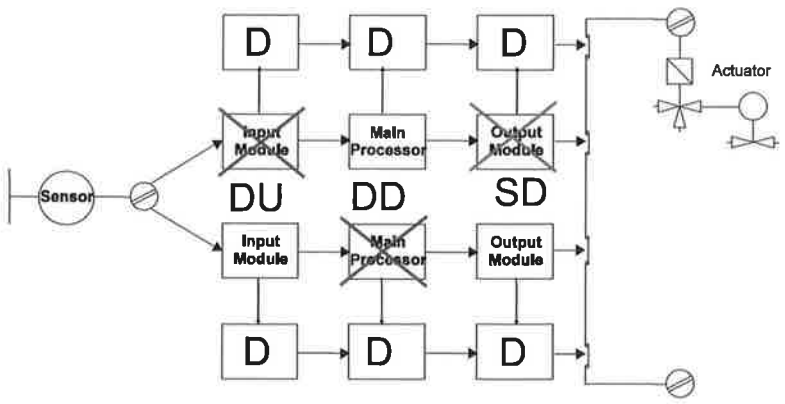
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

1oo2 Safety Instrumented System



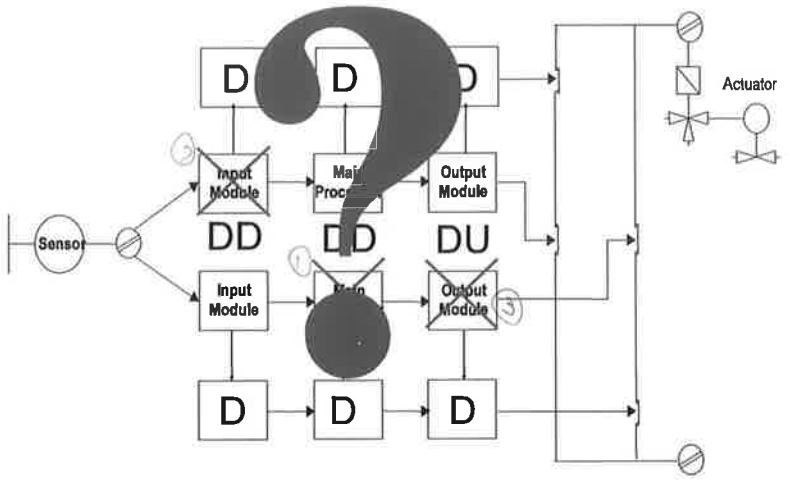
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

1oo2 Safety Instrumented System Version II



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

1oo2 Safety Instrumented System Version III

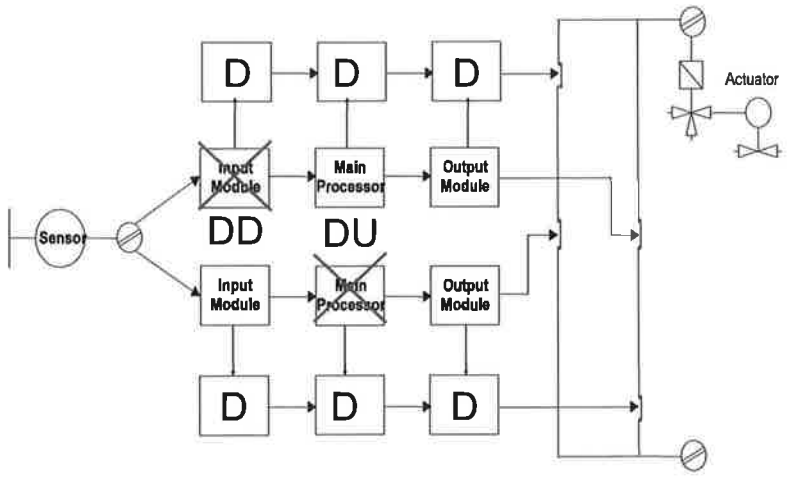


RISKNOWLOGY®

247

Copyright © 2002 - 2011 Risknowlogy®, All rights reserved

1oo2 Safety Instrumented System Version IV



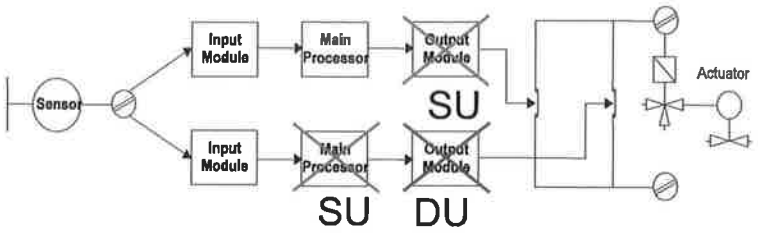
RISKNOWLOGY®

248

Copyright © 2002 - 2011 Risknowlogy®, All rights reserved

2oo2 Safety Instrumented System

- Bad safety system design
  - No safety -> Process Availability



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 11

- Design two SIFs

Subsystem	Type	SFF	HFT	Architecture	Remarks

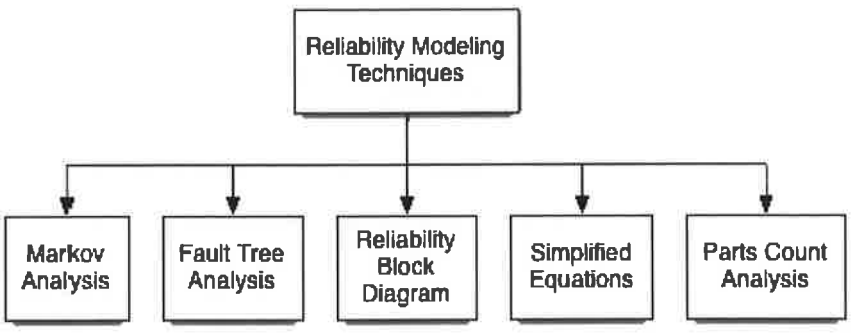
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Reliability Analysis

- Why a reliability analysis? According to the standards we need to
  - Document the failure behavior of the safety function
  - Determine the SFF per subsystem
  - Determine the target failure measure (PFDavg, PFH) per safety function
- Another reason to carry out a reliability analysis
  - Process owner / user also want to know the spurious trip level of the safety function

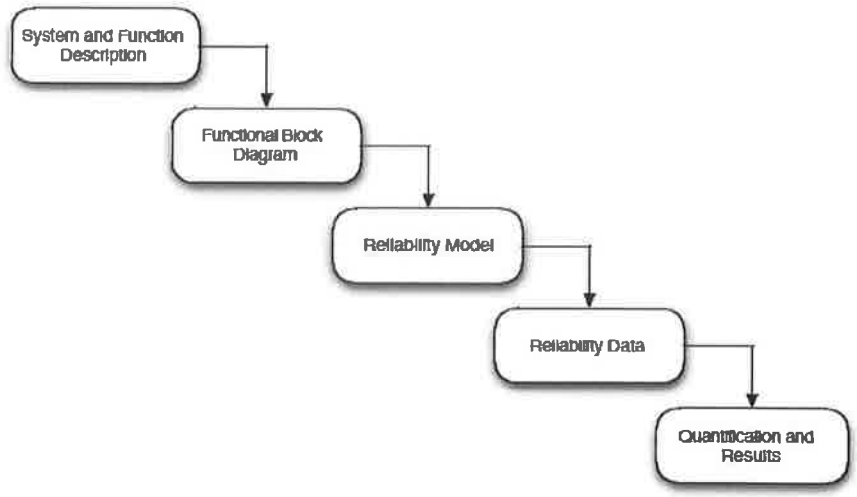
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Reliability Model



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

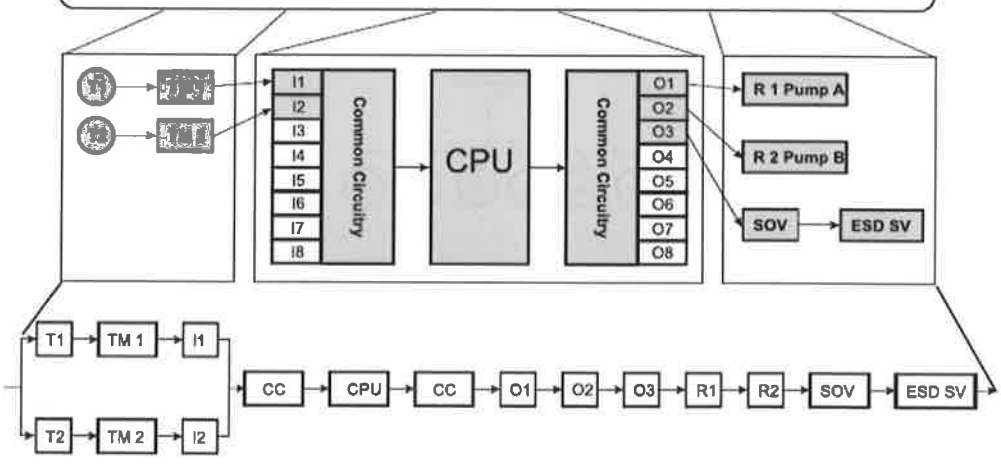
Reliability Analysis Steps



Copyright © 2002 - 2011 Riskonology®. All rights reserved.

From Safety Function to Block Diagram

Measure the temperature and when the temperature exceeds 65 °C open the drain and stop the supply pumps to the reactor within 3 seconds. The function needs to be carried out on SIL 3 level



Copyright © 2002 - 2011 Riskonology®. All rights reserved.

Examples Simplified Equations

- 1oo1

$$PFD_{avg} = (\lambda_{du} + \lambda_{dd}) \cdot t_{CE}$$

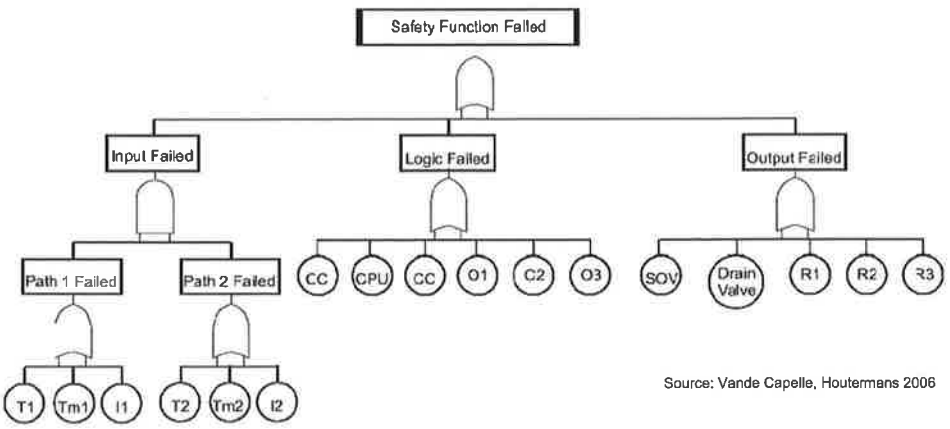
- 1oo2

$$PFD_{avg} = 2\left((1-\beta_D)\lambda_{dd} + (1-\beta)\lambda_{du}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{dd} MTTR + \beta\lambda_{du}\left(\frac{T_1}{2} + MTTR\right)$$

- Don't forget, simplified equations are not that simple, they are derived from Markov models!
- IEC 61508 has formulas for 1oo1, 1oo2, 1oo2D, 2oo2, and 2oo3
  - They are not normative

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Fault Tree Analysis - FTA

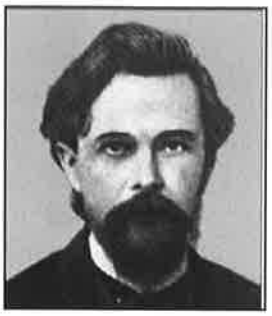


Source: Vande Capelle, Houtermans 2006

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Markov Analysis

- Markov is the most flexible, the most systematic and the only fully traceable reliability technique
- What is Markov about?
  - A.A. Markov - Russian mathematician (1856 – 1922)
  - Involved in random processes
  - Can be applied to systems that behave randomly in time
  - Sounds complicated, but …



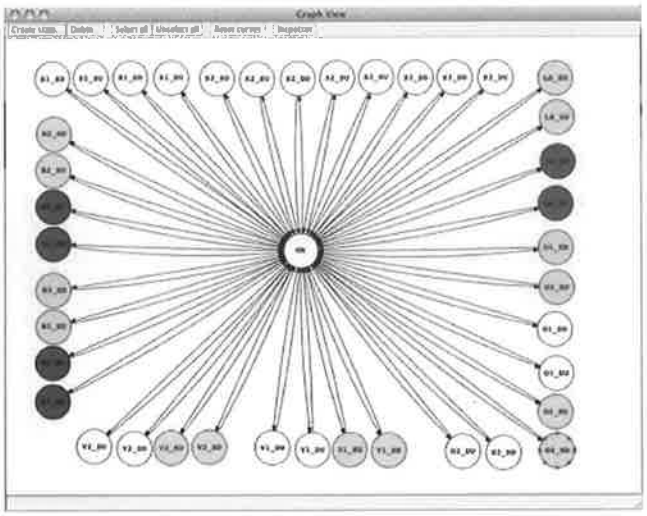
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Markov Modeling

- With Markov you can make 1 model taking into account:
  - Any component with any failure modes (hardware, software, human error, etc)
  - Diagnostic features
  - Repair and test strategies
  - (Im)perfect proof testing
  - Sequences of failures
  - Common cause and systematic failures
  - All of the above in one model and as function of time
- Tools are available that support the model creation and that can solve the Markov model

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

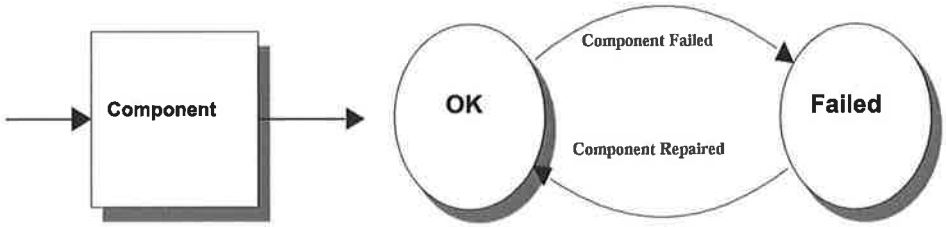
Practical Example of a 2oo3 HIPPS



Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

How to Make a Markov Model

- Markov models consists of
  - Markov states
  - Transitions
    - A working component fails
    - A failed component is repaired



Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

Reliability Data Requirements

- A reliability model is nice but without data we cannot perform any calculations
- We need data on device/equipment level:
  - Safe detected failure rate - SD
  - Safe undetected failure rate - SU
  - Dangerous detected failure rate - DD
  - Dangerous undetected failure - DU
  - Repair times
  - Proof test interval and coverage

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Example Failure Rate Data

- If we have the basic reliability data, for example:
  - SD = 3,06432e-6
  - SU = 1,72368e-6
  - DD = 1,22472e-6
  - DU = 2,8728e-7
  - Mean time to repair = 8 hours
  - Proof test interval = 6 month
  - Proof test coverage = 90%
- Then with the appropriate reliability model we can calculate all important functional safety parameters: SFF, PFDavg, PFH, PFS
- But how do we get the data?

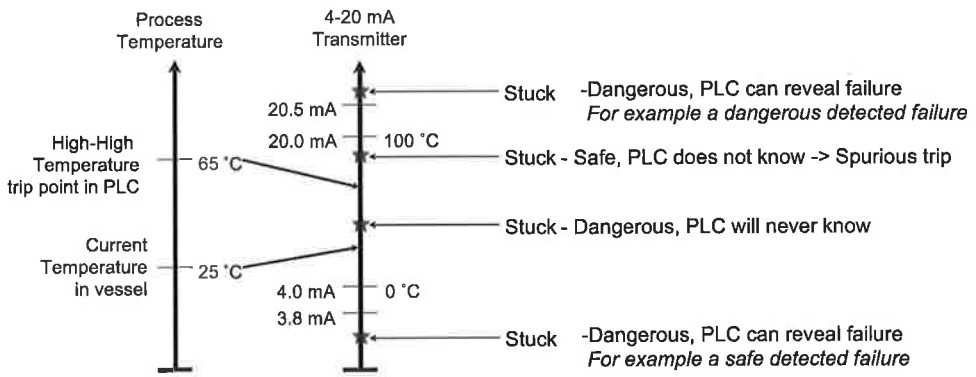
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

How Do We Get the Data?

- For new products we need to perform a reliability study
  - Electronics hardware
  - Mechanical hardware
  - Electro-mechanical hardware
- Most critical aspect of a reliability study is to define the safety function on device level
  - Measure the temperature with an accuracy of ±2% and provide the logic solver with the correct value. If an internal safe failure occurs drive the output signal according to user settings either below 4 mA or above 20mA

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Temperature Transmitter


Process Temperature
4-20 mA Transmitter
20.5 mA
20.0 mA
100 °C
High-High Temperature trip point in PLC
65 °C
Current Temperature in vessel
25 °C
4.0 mA
0 °C
3.8 mA
Stuck -Dangerous, PLC can reveal failure
For example a dangerous detected failure
Stuck - Safe, PLC does not know -> Spurious trip
Stuck - Dangerous, PLC will never know
Stuck -Dangerous, PLC can reveal failure
For example a safe detected failure

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Safety Function of a Device

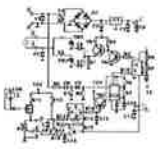
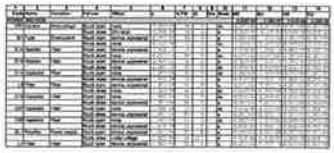
- If we had to buy a temperature sensor, what safety function should it have so that it meets our expectations for the top level end-user safety function?
  - Measure the temperature with an accuracy of +-2% and provide the logic solver with the correct value. If an internal safe failure occurs drive the output signal to below 3.6 mA, if an internal dangerous failure occurs, drive the output signal to above 21 mA

- Lets assume we need to build a SIL 2 temperature transmitter

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Carrying Out an FMEDA

- The developers will perform an FMEDA on the design of a safety device

- Which failure modes to take into account?
  - See table A1 of part 2
- How to build diagnostics for these failure modes?
  - See tables A2 – A14 part 2

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Which Failure Modes Apply?

Components	Requirements for diagnostic coverage or safe failure fraction		
	Low (60%)	Medium (90%)	High (99%)
Discrete hardware			
Digital I/O	Stuck-at	DC fault model	DC fault model drift and oscillation
Analogue I/O	Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Power supply	Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation
Bus			
General	Stuck-at of the addresses	Time out	Time out Wrong address decoding
Memory management unit Direct memory access	Stuck-at of data or addresses No or continuous access	Wrong address decoding DC fault model for data and addresses	All faults which affect data in the memory Wrong data or addresses Wrong access time
Bus-arbitration	Stuck-at of arbitration signals	Wrong access time No or continuous arbitration	No or continuous or wrong arbitration

Source: table A.1 - IEC 61508 part 2

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example FMEDA Data Sheet

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Code	Name	Function	Failure	Effect	e	% FM	D	Dia	Mode	SD	SU	DD	DU
POWER SECTION													
VR1	Varistor	Overvoltage	Stuck open	none	7.00E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
			Stuck close	24V-short	7.00E-09	50	0		s	0.0E+00	3.5E-09	0.0E+00	0.0E-00
SI1	Fuse	Overcurrent	Stuck open	device unpowered	2.50E-08	50	0		s	0.0E+00	1.2E-08	0.0E+00	0.0E-00
			Stuck close	none	2.50E-08	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
R1A	Resistor	Filter	Stuck open	device unpowered	2.00E-10	50	0		s	0.0E+00	1.0E-10	0.0E+00	0.0E-00
			Stuck close	none	2.00E-10	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
R1B	Resistor	Filter	Stuck open	device unpowered	2.00E-10	50	0		s	0.0E+00	1.0E-10	0.0E+00	0.0E-00
			Stuck close	none	2.00E-10	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
C1A	Capacitor	Filter	Stuck open	none	2.00E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
			Stuck close	device unpowered	2.00E-09	50	0		s	0.0E+00	1.0E-09	0.0E+00	0.0E-00
L9	Filter	Filter	Stuck open	device unpowered	1.50E-09	50	0		s	0.0E+00	7.5E-10	0.0E+00	0.0E-00
			Stuck close	none	1.50E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
C18	Capacitor	Filter	Stuck open	none	2.00E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
			Stuck close	device unpowered	2.00E-09	50	0		s	0.0E+00	1.0E-09	0.0E+00	0.0E-00
C67	Capacitor	Filter	Stuck open	none	2.00E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
			Stuck close	device unpowered	2.00E-09	50	0		s	0.0E+00	1.0E-09	0.0E+00	0.0E-00
C68	Capacitor	Filter	Stuck open	none	1.00E-09	50	0		dc	0.0E+00	0.0E+00	0.0E+00	0.0E-00
			Stuck close	device unpowered	2.00E-09	50	0		s	0.0E+00	1.0E-09	0.0E+00	0.0E-00
GL1	Rectifier	Power supply	Stuck open	device unpowered	1.00E-08	50	0		s	0.0E+00	5.0E-09	0.0E+00	0.0E-00
			Stuck close	undervoltage	2.00E-08	50	100		d	0.0E+00	0.0E+00	1.0E-08	0.0E-00
L1	Filter	Filter	Stuck open	device unpowered	1.50E-09	50	0		s	0.0E+00	7.5E-10	0.0E+00	0.0E-00

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Measures to Control Failures

- The outcome of the FMEDA is meaningless if the measures to control failures have not been applied
- Measures to control failures are mainly implemented to deal with random failures
  - They can also support systematic failures.
  - See table A15-A17 of part 2 IEC 61508
- Measures to avoid failures are mainly implemented to deal with systematic failures
  - See tables B1-B5 of part IEC 61508
- These measures help during hardware design and improve the device or product

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Measures to Control Failures

Techniques and measures to control systematic by hardware design failures

Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
Program sequence monitoring	HR	HR	HR	HR
Failure detection by on-line monitoring	R	R	R	R
Test by redundant hardware	R	R	R	R
Standard test access port and boundary-scan architecture	R	R	R	R
Code protection	R	R	R	R
Diverse hardware	-	-	R	R

Techniques and measures to control systematic operational failures

Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
Modification protection	HR	HR	HR	HR
Failure detection by on-line monitoring	R	R	R	R
Input acknowledgement	R	R	R	R
Failure assertion programming	R	R	R	R

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 12

- Once the end-user has defined the safety function, devices and components that can perform this function need to be selected
- Can you define the safety function of
  - A digital logic solver give alarm
  - A power supply feeding the logic solver To be disengaged incase failure
  - A safety relay
  - An emergency shutdown valve

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Exercise # 13

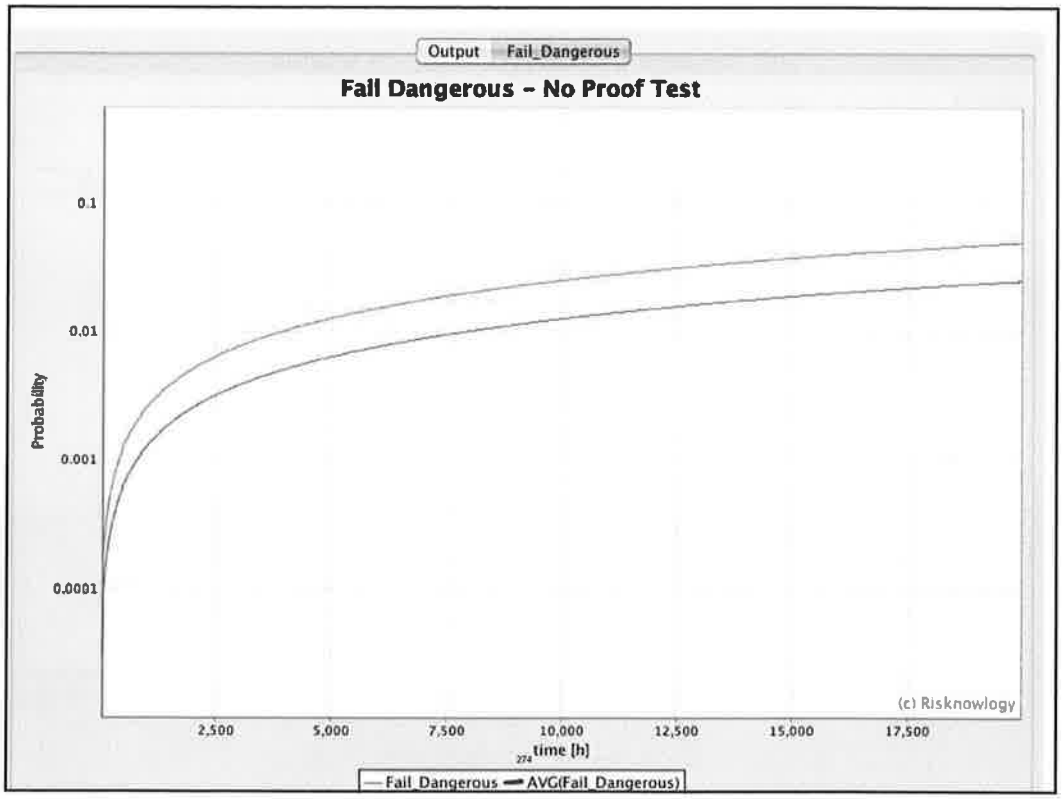
- An accident animation is shown
  - Document what goes wrong
  - And how it could have been prevented
- Lets take a look at what happened

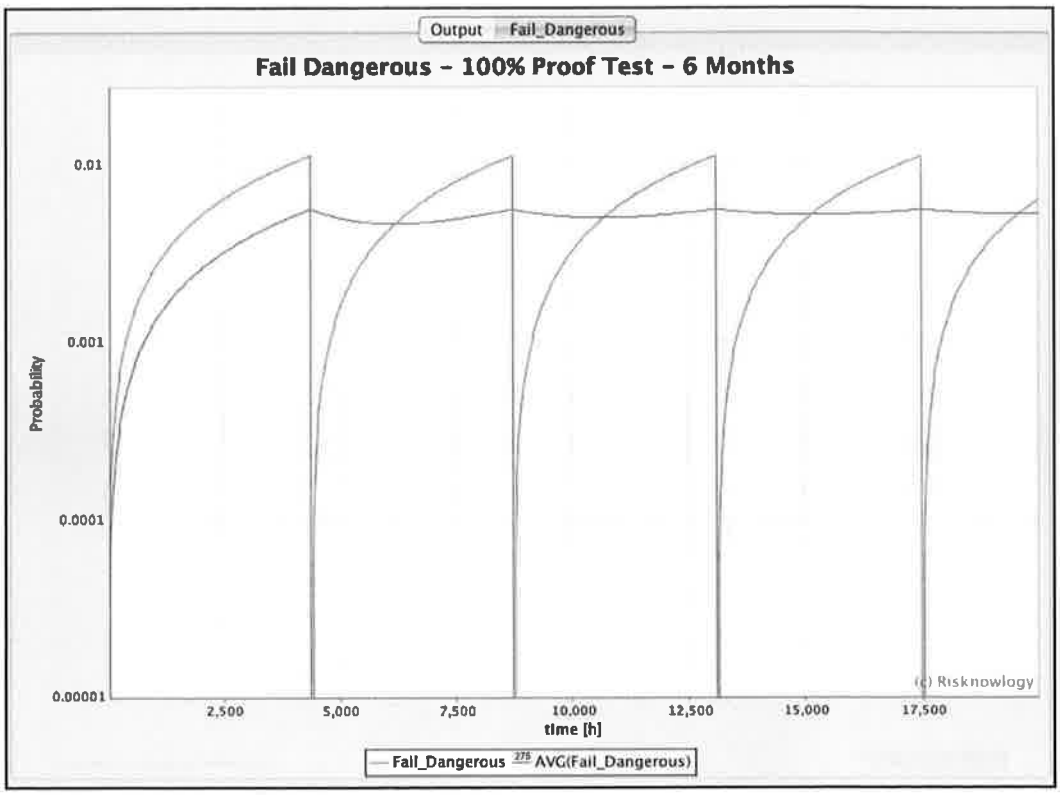
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

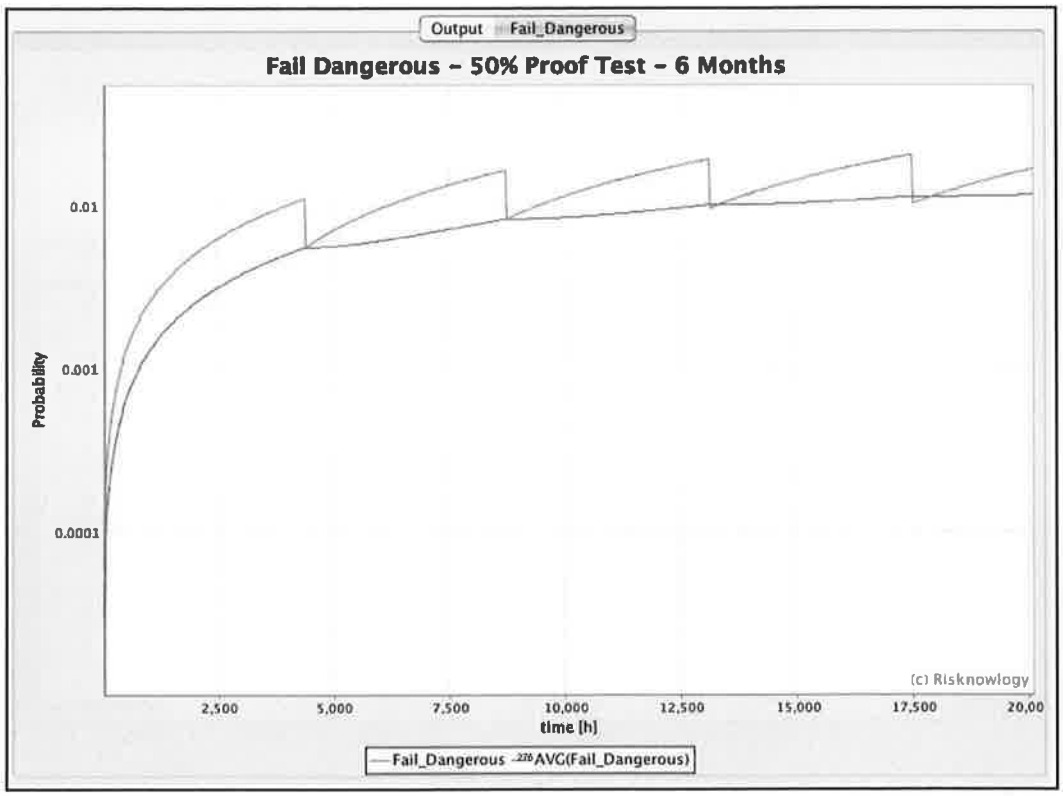
Are You Ready for the PFD Calculation?

- At this point
  - We have the safety function
  - We created a hardware architecture
  - We created a reliability model
    - Markov, FTA, simplified equations, RBDs
  - We performed FMEAs on each safety device
  - We collected the data
  - Now we can perform the PFD calculation

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.



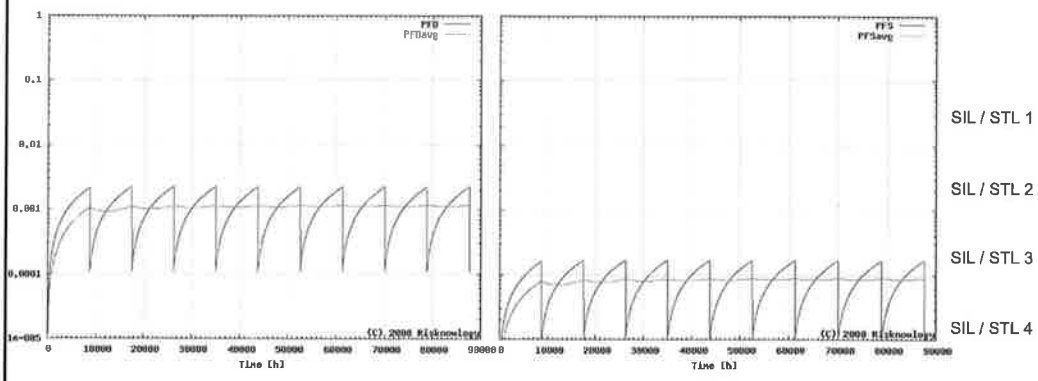

Output Fail_Dangerous
Fail Dangerous - 100% Proof Test - 6 Months
Probability
0.01
0.001
0.0001
0.00001
2,500
5,000
7,500
10,000
12,500
15,000
17,500
time [h]
(c) Risknowlogy
Fail_Dangerous AVG(Fail_Dangerous)


Output Fail_Dangerous
Fail Dangerous - 50% Proof Test - 6 Months
Probability
0.01
0.001
0.0001
2,500
5,000
7,500
10,000
12,500
15,000
17,500
20,00
time [h]
(c) Risknowlogy
Fail_Dangerous AVG(Fail_Dangerous)

Example 2oo3 Safety Function

PFD

PFS



SIL / STL 1

SIL / STL 2

SIL / STL 3

SIL / STL 4

RISKNOWLOGY®

277

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Reliability Calculation Tools

- Many tools are on the market that support reliability calculations
  - Without a formal degree in reliability engineering you can make calculations
  - Most tools support only simplified PFDavg calculations
- Expert tools exist for more advanced calculations
  - PTC - Relex
  - Isograph - Reliabity Workbench
  - Item software - Item Toolkit
  - Risknowlogy - Markov

RISKNOWLOGY®

278

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Summary Module 5

- What did we learn?
  - Important design concepts like HFT, SFF, PFD, low, high demand, energize, de-energize to trip, etc
  - Most important reliability techniques
  - Reliability modeling
  - Reliability calculations

Copyright © 2002 - 2011 Riskonology®. All rights reserved.

Software Design

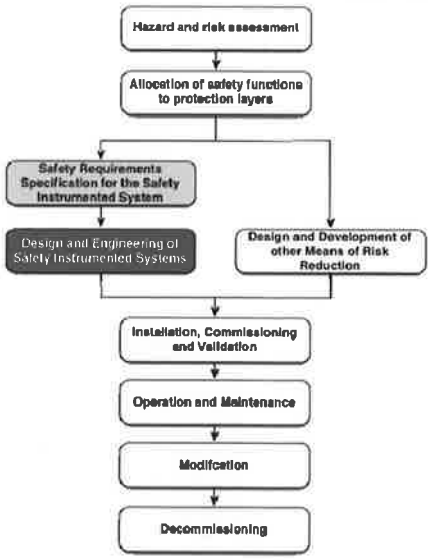
Copyright © 2002 - 2011 Riskonology®. All rights reserved.

Software Design

- In this module
  - Software lifecycle
  - Hardware software relationship
  - A typical software problem
  - Safe software
  - Three types of software
  - Three types of development languages
  - Software tools

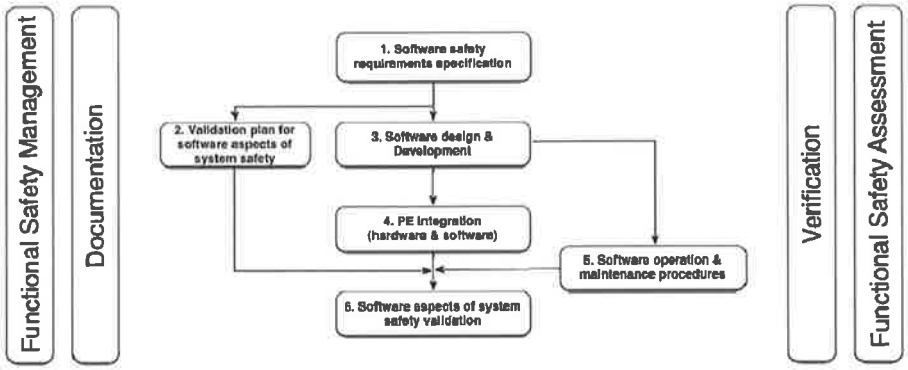
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Where Are We?


Hazard and risk assessment
Allocation of safety functions to protection layers
Safety Requirements Specification for the Safety Instrumented System
Design and Engineering of Safety Instrumented Systems
Design and Development of other Means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning

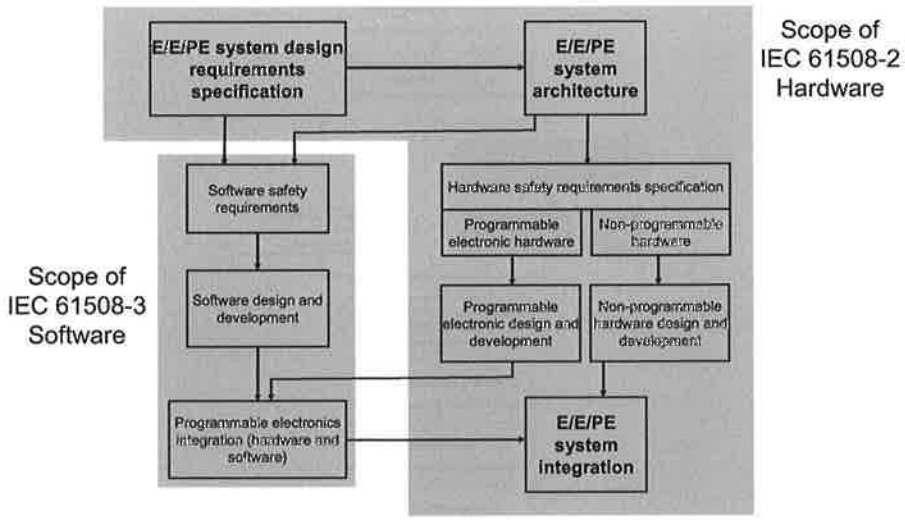
Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Software Lifecycle - IEC 61508


Functional Safety Management
Documentation
1. Software safety requirements specification
2. Validation plan for software aspects of system safety
3. Software design & Development
4. PE integration (hardware & software)
5. Software operation & maintenance procedures
6. Software aspects of system safety validation
Verification
Functional Safety Assessment

Copyright © 2002 - 2011 Riskowlogy®. All rights reserved.

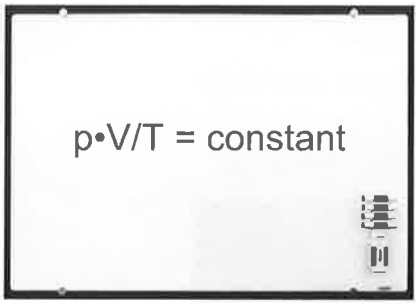
Hardware - Software Relationship


E/E/PE system design requirements specification
E/E/PE system architecture
Scope of IEC 61508-2 Hardware
Software safety requirements
Hardware safety requirements specification
Programmable electronic hardware
Non-programmable hardware
Scope of IEC 61508-3 Software
Software design and development
Programmable electronic design and development
Non-programmable hardware design and development
Programmable electronics integration (hardware and software)
E/E/PE system integration

Copyright © 2002 - 2011 Riskowlogy®. All rights reserved.

An Example

- Client orders a piece of software



Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

An Example

- In the specification is written:

Specification

Req. 1.2.83:

Calculate pressure with following formula

$$p = c \cdot V / T$$

Copyright © 2002 - 2011 RiskNowlogy®. All rights reserved.

An Example

- The programmer in the mean time…
  - Programs formula according to requirement: 1.2.83
  - Tests requirement: 1.2.83
  - Delivers a finished and test program according to specification

Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

An Example

- What can go wrong?
  - Is the specification correct?
    - No, actually not: $p \cdot V / T = \text{const} \neq p = c \cdot V / T$
  - Was the program correct?
    - Yes, the test showed it was correct
  - Was the test correct?
    - Yes, the result look good
  - Was the test verified?
    - Yes, the creator of the test verified it
  - Did we actually do the test?
    - Yes, I signed the paper, didn't I!

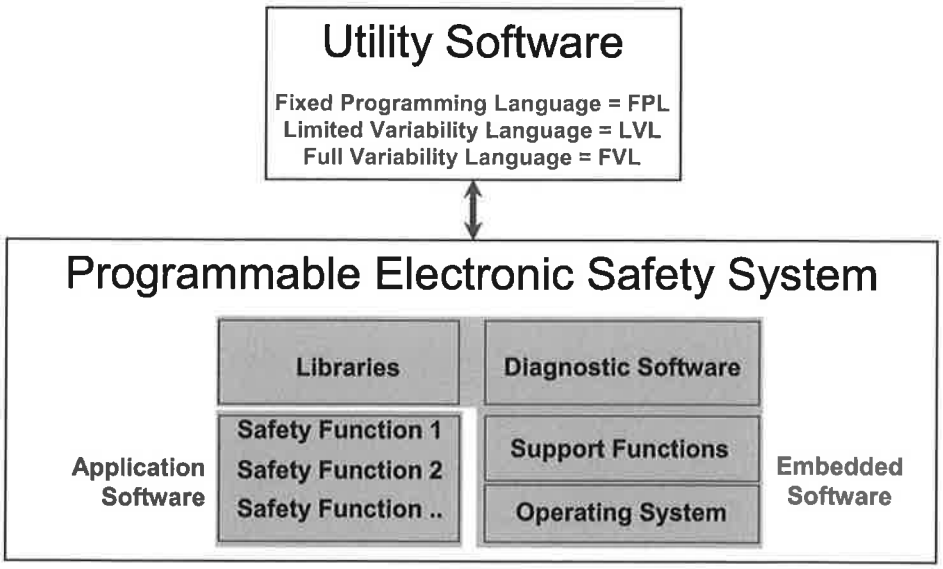
Copyright © 2002 - 2011 Riskonowlogy®. All rights reserved.

Safe Software Is Needed

- What we need to achieve is ***safe*** software...
  - Software is safe if
    - The safety system can execute the safety function even under faulty conditions
    - It can handle software bugs as well as hardware failures
    - It has been developed according to functional safety standards
- Features to achieve safe software are mainly built on embedded software level IEC 61508 world
- On application level we mainly deal with relative simple software logic IEC 61511 world

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Embedded, Application and Utility Software



Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Three Types of Development Software

- IEC 61508 deals with
  - Full variability languages (FVL)
    - C, C++, Assembler, Etc.
    - Good engineering practices
    - Measures to avoid failures - Tables in part 3
- IEC 61511 deals with
  - Limited variability languages (LVL)
    - Function blocks, ladder logic, etc.
  - Fixed programming languages (FPL)
    - A sensor with only an up and down button to set a limit

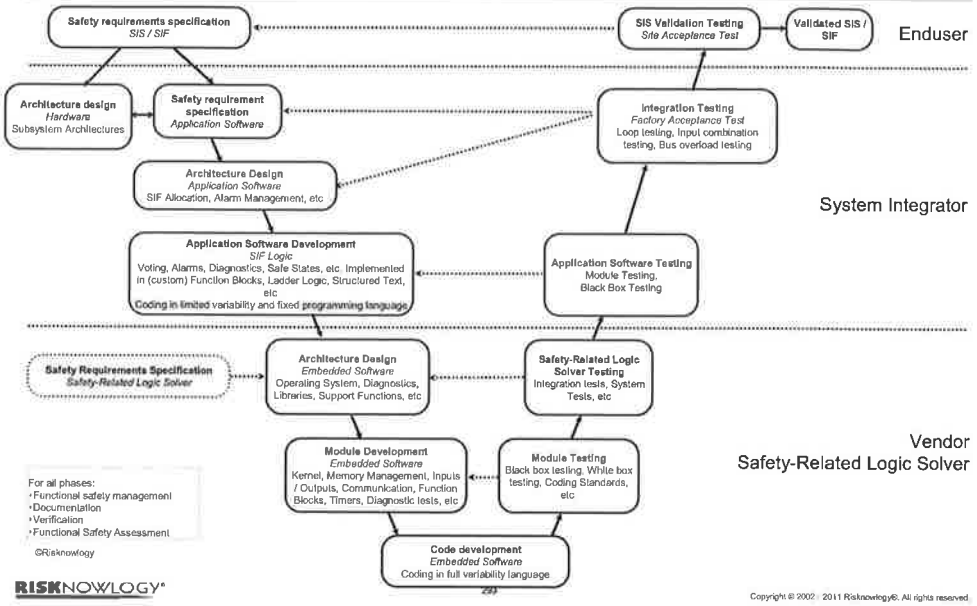
Copyright © 2002 - 2011 Risknowlogy®, All rights reserved

IEC 61511 Software

- IEC 61511
  - Does not differentiate between SIL 1, 2 or 3 software
  - Lists requirements which are suitable for up to SIL 3
  - Does not allow SIL 4 software but refers in that case back to IEC 61508
- Software can be developed according to the V-model

Copyright © 2002 - 2011 Risknowlogy®, All rights reserved

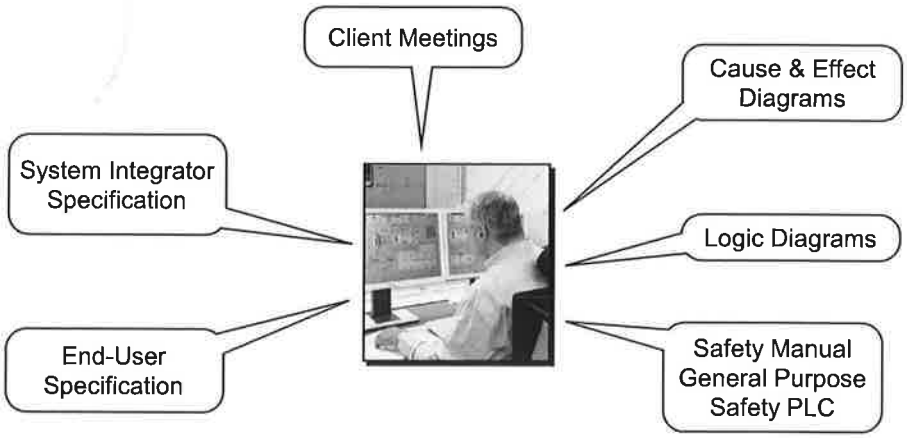
Software Management via V-model



RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Application Software Development



And where is the Software Safety Requirements Specification?
If you do not have one, the software engineer will use his own interpretation

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved

Application Software

- Application software can include
  - Logic in terms of voting blocks
  - Limits in terms of settings
  - Timing elements
  - Bypass logic
  - Diagnostics, alarms and associated safe state actions
    - To maintain architectural constraints as defined in the SRS
- Remember
  - Software should be based on a software safety requirements specification
  - Software not only influences safety availability but also process availability
  - Software means dealing with systematic failures

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Application Software Testing

- Bad example
  - Print out the logic
  - Test the logic by "line by line" review
  - What did we proof now? That the printer did not make a mistake?
- Better example
  - Compare programmed logic to the software requirements specification
  - Test each individual loop (FAT/SAT)
  - Test all possible input combinations and monitor all outputs with an event logging tool (FAT/SAT)
  - Perform tests like communication overload, short circuits on signal lines, etc and verify correct working of diagnostics, alarms, voting and safe state actions

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Measures to Avoid & Control Failures

- The measures
  - Are grouped according to lifecycle phases
  - The effectiveness of the measures is determined by SIL
  - Only failures that have occurred we can try to control
  - See tables A1-A10 and B1-B9 in part 3 IEC 61508

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Measures to Avoid Failures

Software design and development - detailed design

	Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
1a	Structured methods	HR	HR	HR	HR
1b	Semi-formal methods	R	HR	HR	HR
1c	Formal design and refinement methods	---	R	R	HR
2	Computer-aided design tools	R	R	HR	HR
3	Defensive programming	---	R	HR	HR
4	Modular approach	HR	HR	HR	HR
5	Design and coding standards	R	HR	HR	HR
6	Structured programming	HR	HR	HR	HR
7	Use of trusted/verified software elements (If	R	HR	HR	HR
8	Forward traceability between the software safety requirements specification and software design	R	R	HR	HR

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Measures to Control Failures

- Software is written to deal with random failures
- Measure to control failures include for example:
  - Hardware architecture
  - Self test measures for system and sub–systems
    - CPU
    - Bus and signal
    - RAM, EEPROM, ROM, flash
  - System watchdog with independent time base
  - Program flow monitoring
  - Safety protocols for data transmission paths
  - Redundant and/or inverse data storage

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Summary Module 6

- What did we learn…
  - Software safety is more about the process of software development than the software itself
  - Systematic approach via V-model
  - Measure to control and avoid failures need to be applied

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Certification, Proven In Use, and Data

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Certification, Proven In Use, and Data

- In this module
  - Dilemma for end users and system integrators
  - What is certification
  - What to look for in a certificate
  - What is proven in use
  - How to prove "proven in use"
  - Reliability data sources

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Dilemma for End-Users and SI

- Often heard comment:
  - "I cannot analyze in detail each hardware and software aspect of a device. I am a process control engineer. Not a circuit diagram designer or a programmer of operating systems. How do I know these devices are compliant?"
  - "Our plant has been running fine for 10 years. Why should I replace all my working equipment with new safety equipment?"

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

IEC 61508 Compliant Devices

- A device is fully compliant with IEC 61508 when the following requirements have been addressed
  - ☑Functional safety management
  - ☑ Hardware requirements
  - ☑ Hardware reliability analysis
  - ☑ Software requirements
  - ☑ Basic electrical safety, EMC, environmental
  - ☑ User documentation
- How many products do you know that are fully compliant?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

How Do You Know Everything Is Compliant?

- Help is on the way! as an user
  - You do not need to analyze products in detail
  - You can make use of
    - Certified devices and/or
    - Proven in use devices and/or
    - Existing reliability data sources
- You only need to understand how to apply the above options

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Certification

- What is certification?
  - Somebody who certifies attests that a statement made is true
  - For example to attest that the IEC 61508 standard has been met for the smart transmitter
- Certification is NOT required by IEC 61511
  - The word certification does not exist in IEC 61511
  - IEC 61511 only knows verification, validation, assessment, and audits
- How it helps?
  - If a product, system, organization or person is certified
    - You have less analyses and verification to do
    - You have less of a headache!
    - Because somebody else did the work for you

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What to Look for in a Certificate…

- A good certificate should state
  - The manufacturer and the certified product(s)
  - The main standards applied
  - The level of safety achieved
  - The corresponding report to the certificate and the safety manual
- The report to the certificate should
  - Explains how and what has been certified
  - Should lists restrictions on use, if any
- The safety manual should explain how to install, commission, operate, maintain, and repair the safety device
- Do not buy a product unless you first received the **certificate + report + safety manual**

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Certificate Product

CERTIFICATE

Holder of Certificate: ABB AB, Open Control Systems
SE/PA/AVA
Tvärleden 2
721 59 Västerås
SWEDEN

Product: **Safety Related Programmable Electronic System**

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be altered in any way. See also notes overleaf.

Model(s): **800xA Safety**

Parameters: Logic solver: AC 800M High Integrity (HI) comprising
PM865 and SM810 - SIL 1-2, CAT 3, PL e
PM865 and SM811 - SIL 1-3, CAT 4, PL e
I/O modules: AI880A, DI880, DO880 - SIL 1-3, CAT 4, PL e

Further approvals can be found in the report referenced below.

The report referenced below and the user documentation in the currently valid revision are mandatory part of this certificate. The product complies with the following listed safety requirements only if the specifications documented in the currently valid revisions of this report are met.

Test report no.: AO 63111 C

CERTIFICATE

Holder of Certificate: HYDAC SYSTEM GmbH

Product: **Safety-, control- and regulator equipment 2oo3 Safety Control Block**

Model(s): **EHS 2v3-10-PSH-XX-XX/EX1-XX-NA-XXXX-XXX-XXX-XX**
EHS 2v3-10-PSA-XX-XX/EX1-XX-NA-XXXX-XXX-XXX-XX
EHS 2v3-10-PSO-XX-XX/EX1-XX-NA-XXXX-XXX-XXX-XX
For nomenclature see attachment

Parameters:

Solenoid voltage	24 VDC
Operating pressure range	8-66 bar
Max. static operating pressure	160 bar
Ambient-temperature range	-20°C +70°C

Tested according to: IEC 61508 2000 Part 1 to 7 (SIL 3, Low- and High Demand Mode)
IEC 61511 2004

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: HS82358T

RISKNOWLOGY®
308

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Certificate, Report + Safety Manual

RISKNOWLOGY

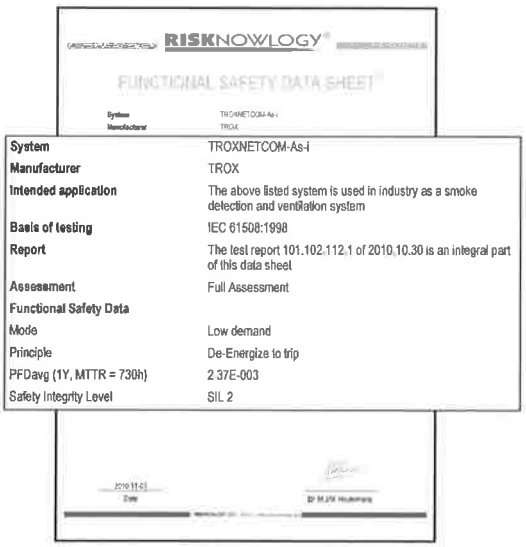
+

Technical Report
Proven in Use – SITRANS LR250 (HART)

+

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Loop Certification


RISKNOWLOGY

FUNCTIONAL SAFETY DATA SHEET

System	TROXNETCOM-As-i
Manufacturer	TROX
Intended application	The above listed system is used in industry as a smoke detection and ventilation system
Basis of testing	IEC 61508:1998
Report	The test report 101.102.112.1 of 2010.10.30 is an integral part of this data sheet
Assessment	Full Assessment
Functional Safety Data	
Mode	Low demand
Principle	De-Energize to trip
PFDavg (1Y, MTTR = 730h)	2.37E-003
Safety Integrity Level	SIL 2

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Organization

TÜVRheinland®

The company

HIMA Paul Hildebrandt GmbH + Co KG
Projektmanagement und Engineering
Industrie-Automatisierung
Albert-Bassermann-Straße 28
68782 Brühl

HIMA

TÜVRheinland FSM

has proven successfully within the scope of an audit that a Functional Safety Management System (FSM-System) has been introduced and applied accordingly.

Object of the audit is the proof of implementation of the requirements defined in the basic standards relating to the **Management of Functional Safety**, the **Documentation**, the **Functional Safety Assessment** as well as the **company specific Safety Lifecycle Phases** according to the scope of certification.

IEC 61508: E/E/PE- safety related System Integration
IEC 61511: SIS - Integration

Object of the Scope of Certification is the integration of E/E/PE-safety related Systems, Sensors and Actuators respectively SIS and comprises their configuration, application programming, assembly, and test as well as safety loop calculations for specific industrial safety applications.

The audited FSM-System and its involved company departments fulfill the organizational premises for the listed Scope of Certification.

Valid to: ... August 2012

Cologne, 2010-01-08

TÜV Rheinland Industrie Service GmbH

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Example Certification People

RISKNOWLOGY®

CERTIFICATE

John Doe

Has successfully completed the Functional Safety Certification Program requirements for

Functional Safety Professional

In accordance with
IEC 61508:2010

Date issued 2010-12-06
ID number TP10050101
Field Safety Industry
Subject Safety-Related Systems

G. Greil
Certifier

Dr. M. Houtermans
Trainer

CERTIFICATE

Dr. Michel Houtermans

Has successfully completed the Functional Safety Certification Program requirements for

Functional Safety Expert

In accordance with
IEC 61508:1998
IEC 61511:2003

ID number TP08000101
Field Process industry
Subject Functional safety management
Hardware and software design
Safety instrumented systems
Date issued 2009-08-04

G. Greil
Certifier

RISKNOWLOGY®

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Who Can Certify?

- In principle any company and/or person in the world can certify
- The question is not "who can certify?"
  but "who do you trust?"
- Much more important then who can certify is to pay attention to
  - **WHAT** has been certified, and
  - **HOW** has it been certified

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Questions

- What is the difference between a device that is certified and a device that is not certified?
- Is certification always complete?
- Can proven in use be certified?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

Proven In Use

- "Proven in use" is defined by IEC 61511 as
  - When a **documented** assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system
    - The evidence is dependent on the complexity of the device and the target failure measures
- Why is it so tempting to apply?
  - Because if a subsystem is regarded as proven in use, then, information regarding the measures and techniques for the prevention and control of systematic faults is not required (i.e., Tables in IEC 61508 part 2 and 3)
  - Failure rate data is still required!

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

What Actually Needs to Be Proven?

- So what is it that we try to prove?
  - The most important evidence is that the actual safety function of the safety device or subsystem executes as designed
  - If we cannot proof, with documented evidence, that the safety function works, we cannot claim proven in use
- For example
  - Consider the safety function of an emergency shutdown valve, i.e., close upon demand
    - If an ESD valve was installed for 5 years but had never been closed we cannot know whether it works when needed.
    - We cannot claim proven in use evidence as it was never used
    - How can we collect evidence?

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

How to Prove "Proven in Use"

- Evidence for proven in use must be documented
- Evidence needed:
  - The element / subsystem has restricted functionality
    - A PLC can never be claimed as proven in use
    - A transmitter can, a relay can, a valve can....
  - Conditions of use are the same or sufficiently close
    - If not the same an impact analysis of the differences must be carried out
  - If functions are present that are not part of proven in use then it needs to be proven that they do not interfere with the proven in use functions
  - Any future modifications to a proven in use element / subsystem needs to follow the modification procedures

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.

How to Prove "Proven in Use"

- Evidence needed
  - Evidence is based on operational experience
  - The volume of the considered operating experience has a minimum of 70 % confidence interval
  - Statistical evidence that the claimed dangerous failure rate is sufficiently low
    - Very difficult to meet as failure track records are usually not available
  - Performance of the components or subsystems in similar operating profiles and physical environments

Copyright © 2002 - 2011 Risknowlogy®. All rights reserved.